4. DATABASE ADMINISTRATION 1

4.1 Product Installation and Disk Storage Management 1
4.1.1 Installing SQL Server and Related Products and Upgrading New Version of SQL Server Products 1
4.1.2 Migrating Databases to New Version SQL Server 1
4.1.3 Allocating Resources 1
4.1.3.1 Creating Database Devices 1
4.1.3.2 Creating User Databases 4
4.1.3.3 Creating Segments 7
4.1.3.4 Creating Dump Devices 10
4.1.4 Monitoring and Managing Resource Utilization 13
4.1.4.1 Use of Available Disk Space, Memory, Connection Error Logs, State of Transaction Logs, Device Problems, etc. 13

4.2 SQL Server Life Cycle Maintenance 13
4.2.1 Create A Managed SQL Server Resource 13
4.2.2 Configure SQL Server 15
4.2.3 Start an SQL Server Process 18
4.2.4 Stop an SQL Server 19

4.3 SQL Server Logins and Privileges 21
4.3.1 Creating SQL Server Login Accounts 22
4.3.2 Add User to Database(s) 25
4.3.3 Granting Access Privileges 27
To grant access privileges, the DBA must have the following TME administrator roles: 27
4.3.4 Modifying Access Privileges 30

4.4 Database Integrity 33
4.4.1 Checking Consistency 33

4.5 Backup and Recovery 33
4.5.1 Database and Transaction Log Backup 33
4.5.2 Database Device Restore 37
4.5.2.1 Examine Space Usage For Each Database on the Failed Device 38
4.5.2.2 Delete Database(s) on Failed Device and Delete the Failed Device 38
4.5.2.3 Re-load Each Database from Database and Transaction Log Backups 40

4.6 ECS DAAC-Configured Databases 45
4.6.1 Database Size Estimates and Planning 45
4.6.2 Database-unique Attributes 45
4.6.3 Database Reports 45

4.7 Database Tuning and Performance Monitoring 45
4.7.1 Design and Indexing 45
4.7.2 Queries 45
4.7.3 Monitoring and Boosting Performance 45

4.8 Troubleshooting 45
4.8.1 Diagnosing Database System Problems 45
4.8.1.1 Reports 45

4.8.1.2 Queries 45
4.8.2 On-call User Support and Emergency Response 45

5. SECURITY SERVICES ERROR! BOOKMARK NOT DEFINED.

5.1 Running Security Log Analyst Program 2

5.2 Generating Security Reports 2

5.3 Running the Network Authentication Service 2

5.4 Monitoring Network Vulnerabilities 4

5.5 Ensuring Password Integrity 4
5.5.1 Detecting Weak Passwords 5
5.5.1.1 Configuring Crack 5
5.5.1.2 Running Crack 6
5.5.1.3 Creating Dictionaries 7
5.5.1.4 Options 7
5.5.1.5 Crack Support Scripts 8
5.5.1.6 Checking the Log 9
5.5.2 Enforcing Strong Passwords 9
5.5.2.1 Configuring npasswd 9
5.5.2.2 Building npasswd 10

5.6 Monitoring Requests for Network Services 11

5.7 Monitoring File and Directory Integrity 11
5.7.1 Updating the Tripwire Database 12
5.7.1.1 Updating Tripwire Database in Interactive mode 12
5.7.1.2 Updating Tripwire Database in Database Update Mode 12
5.7.2 Configuring the tw.config file 13

5.8 Reporting Security Breaches 14

5.9 Initiating Recovery from Security Breaches 14

6. NETWORK ADMINISTRATION 1

6.1 HPOpenView Network Node Manager (NNM) 1
6.1.1 Starting Network Node Manager (NNM) 2
6.1.2 Creating Additional Objects 3
6.1.2.1 Adding a Network Object 4
6.1.2.2 Adding a Segment Object 5
6.1.2.3 Adding a Node Object 7
6.1.2.4 Adding an IP Interface Object 9
6.1.3 Viewing the Current Network and System Configuration 10
6.1.4 Viewing Network Address Information 11
6.1.5 Viewing How Traffic is Routed on a Network 13
6.1.6 Viewing the Services Available on a Node 14

6.2 Diagnosing Network Problems 16

7. SYSTEM MONITORING 1

7.1 Checking the Health and Status of the Network 1
7.1.1 Starting Network Node Manager (NNM) 2
7.1.2 Verify that an Object Is Not Functioning 3
7.1.3 Looking at Maps for Color Alerts 4
7.1.4 Looking at Maps for New Nodes 5
7.1.5 Creating Special Submaps for Monitoring Status 5
7.1.6 Checking for Event Notifications 5

8. PROBLEM MANAGEMENT 1

8.1 Problem Resolution Process — An Overview 1

8.2 Using the Trouble Ticket System Tool 7
8.2.1 Accessing the Trouble Ticket System 9
8.2.1.1 Remedy's GUI Admin Tool 11
8.2.1.2 Remedy's GUI Import Tool 11
8.2.1.3 Remedy's Hardware Information Schema 11
8.2.1.4 Remedy's GUI Notification Tool 12
8.2.2 Submit a Trouble Ticket 12
8.2.3 Reviewing and Modifying Open Trouble Tickets 13
8.2.4 Forwarding Trouble Tickets 14
8.2.5 Adding Users to Remedy 14
8.2.6 Changing Privileges in Remedy 15
8.2.7 Modifying Remedy's Configuration 16
8.2.8 Generating Trouble Ticket Reports 16
8.2.9 Re-prioritization of Dated Trouble Ticket Logs 16

8.3 Using Hypertext Mark-up Language (HTML) Screens 17
8.3.1 ECS Trouble Ticketing HTML Submit Screen 17
8.3.2 ECS Trouble Ticketing HTML Success Screen 18
8.3.3 ECS Trouble Ticketing HTML List Screen 18
8.3.4 ECS Trouble Ticketing HTML Detailed Screen 19
8.3.5 ECS Trouble Ticketing HTML Help Screen 19

8.4 Emergency Fixes 20

4. Database Administration

4.1 Product Installation and Disk Storage Management

4.1.1 Installing SQL Server and Related Products and Upgrading New Version of SQL Server Products

4.1.2 Migrating Databases to New Version SQL Server

4.1.3 Allocating Resources

4.1.3.1 Creating Database Devices

A database device is created when the System Administrator determines that new disk space is available for use by a Sybase database, as part of the Database Recovery Procedure. The System Administrator makes a request to the DBA who creates the new database device and notifies the System Administrator when the device has been created.

The Activity Checklist table that follows provides an overview of the database device creation process. Column one (**Order**) shows the order in which tasks should be accomplished. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task. Column three (**Task**) provides a brief explanation of the task. Column four (**Section**) provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found. Column five (**Complete?**) is used as a checklist to keep track of which task steps have been completed.

Table 4.1-1 Create Database Device - Activity Checklist

Order	Role	Task	Section	Complete?
1	System Admin.	Confirm Need for a New Database Device	(I) 4.1.3.1	
2	System Admin.	Request creation of Database Device by DBA	(I) 4.1.3.1	
3	DBA	Create New Database Device	(P) 4.1.3.1	
4	DBA	Notify Requester and System Admin. when Database Device is Available	(I) 4.1.3.1	

The procedures assume that the device failure has been verified by the System Administrator. In order to perform the procedure, the DBA must have obtained the following information:

a. Name of database device to create.

b. Physical device on which to place database device.

c. Device size in megabytes.

d. For a mirrored device, name of the mirror device.

To create database devices, the DBA must have the following TME administrator roles:

a. user (TME)

b. space (ESSM)

c. sa_role (SQL Server)

Table 4.1-2 presents the steps required to create a database device in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below:

1 Log into a Tivoli Server by typing: **telnet TivoliServerName** or **rsh TivoliServerName**, then press **Return**.

2 If a **Login**: prompt appears, log in as yourself by typing: **YourUserID**, then press **Return**.

- A password prompt is displayed.

3 Enter **YourPassword**, then press **Return**.

- Remember that **YourPassword** is case sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.

4 Set display to current terminal by typing: **setenv DISPLAY IPNumber:0.0** or **setenv DISPLAY TivoliServerName:0.0**, then press **Return**.

5 Type **tivoli**. Press **return**.

- You will now be in the TME Desktop for Administrator (your name) window.

6 Double-click the **SQL Server** icon in the policy region window to open the SQL Server Window.

7 Double-click the **Database Devices** icon in the SQL Server window to open the Database Devices Manager window.

For each database device to be created, perform steps 8 through 15:

8 From the **Device** menu of the Database Devices Manager window, choose **Create**.

- The Create Database Device dialog box opens. You can now specify the attributes of the new database device.

9 For **Logical Name**, enter the name you want to assign to the device.

10 For **Physical Name**, enter the full path name of the physical device in your environment to which to map the logical name.

11 For Size, enter the device size in megabytes.

12 If you want the device to be a default device, check the **Default Device** box.

*To mirror the device, enter **Disk Mirroring** group box described in steps 13 and 14:*

13 For **Mirror Name**, enter the physical name of the mirror device.

14 Specify whether to use serial or parallel writes by selecting the **Serial** or **Parallel** radio button.

15 Click **Create**.

- SQL Server creates the database device.

16 To close the Database Devices Manager window, choose **Close** from its **Device** menu.

17 To close the SQL Server window, choose **Close** from its **Server** menu.

18 To close the TME Desktop window, choose **Close** from its **Desktop** menu.

19 Confirm the exit by clicking **Yes** in the confirmation dialog box.

20 At the UNIX prompt for the SQL server, type **exit**, then press **Return**.

- You are logged out and disconnected from the Tivoli Server.

Table 4.1-2 Create Database Devices - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	**telnet** *TivoliServerName* **-or-** **rsh** *TivoliServerName*	**press Return**
2	*YourUserID* **-or-** (No entry)	**press Return -or-** (No action)
3	*YourPassword*	**press Return**
4	**setenv DISPLAY** *IPNumber*:**0.0 -or-** **setenv DISPLAY** *TivoliServerName*:**0.0**	**press Return**
5	**tivoli**	**press Return**
6	**Double-click the SQL Server icon**	(No action)
7	**Double-click the database devices icon**	(No action)

	For each device, steps 8-15	
8	**Device Menu → Create**	**press Return**
9	**Name of device**	(No action)
10	**Physical device**	(No action)
11	**Device Size**	(No action)
12	**Optionally, check Default Device**	(No action)
	To mirror the device, steps 13-14	(No action)
13	**Name of mirror device**	(No action)
14	**Serial -or- parallel writes**	(No action)
15	**Click Create**	(No action)
16	**Devices→Close**	**press Return**
17	**Server→Close**	**press Return**
18	**Desktop→Close**	**press Return**
19	**Click Yes**	(No action)
20	**exit**	**press Return**

4.1.3.2 Creating User Databases

A User Database is created when a request is received or as part of the Database Recovery Procedure.

The requester fills out a "User Database Request Form" and submits it to his/her supervisor. The "User Database Request Form" includes information regarding the user (User Name, UNIX ID, Group, Organization, and Site) and databases to be created, and the user's explanation of why a new User Database is needed. The requester's supervisor reviews the request, and if he or she determines that it is appropriate to create the User Database, forwards the request to the Operations Supervisor (Ops Super). The Ops Super verifies that all required information is contained on the form. (Incomplete forms are returned to the requester's supervisor for additional information.) If it is complete and if the request for a new User Database fits within policy guidelines, the Ops Super approves the request and forwards the request form to the DBA to implement After the User Database is created, the DBA notifies the requester that the new database is available. The DBA also sends an e-mail message to the user's supervisor informing him/her that the new User Database has been created.

The Activity Checklist table that follows provides an overview of the user database creation process. Column one (**Order**) shows the order in which tasks should be accomplished. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task. Column three (**Task**) provides a brief explanation of the task. Column four (**Section**) provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found. Column five (**Complete**?) is used as a checklist to keep track of which task steps have been completed.

Table 4.1-3 Creating User Database - Activity Checklist

Order	Role	Task	Section	Complete?
1	System Admin.	Confirm the Need for a User Database	(I) 4.1.3.2	
2	System Admin.	Request Creation of a User Database by DBA	(I) 4.1.3.2	
3	DBA	Create New Database	(P) 4.1.3.2	
4	DBA	Notify Requester and System Admin. when User Database Is Available	(I) 4.1.3.2	

In order to perform the procedure, the DBA must have obtained the following information:

a. Name of database to create

b. Size of database

c. Database devices to use

To create a user database, the DBA must have the following TME administrator roles:

a. space (ESSM)

b. sa_role (SQL Server)

Table 4.1-4 presents the steps required to create a user database in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below:

1 Log into a Tivoli Server by typing: **telnet TivoliServerName or rsh TivoliServerName**, then press **Return**.

2 If a **Login:** prompt appears, log in as yourself by typing: **YourUserID**, then press **Return**.

- A password prompt is displayed.

3 Enter **YourPassword**, then press **Return**.

- Remember that YourPassword is case sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.

4 Set display to current terminal by typing: **setenv DISPLAY IPNumber:0.0** or **setenv DISPLAY TivoliServerName:0.0**, then press **Return**.

5 Type **tivoli**. Press **return**.

- You will now be in the TME Desktop for Administrator (your name) window.

6 Double-click the **SQL Server** icon in the policy region window to open the SQL Server Window.

7 From the **Database** menu of the SQL Server Window, choose **Create**.

- The Create Database dialog box opens. You can now specify the attributes of the new database.

8 For **Name**, enter the name of the database to create.

9 For **Owner**, enter the SQL Server login name of the database owner.

10 If you are creating the database so you can restore it from a backup, check the **For Load** check box.

In the Database Devices group box, enter specifications for how to allocate the database on one or more devices. For each database device allocation, execute steps 11-14:

11 Select the **name** of a database device from the Name drop-down list box.

12 Enter the size of the allocation on the device in the **Size** edit box.

13 To allocate a device to the transaction log on a separate device from the data, select the **Log** option button.

14 Click the **Add** button to transfer the allocation information into the list of database devices allocated for this database.

15 Click the **OK** button.

- SQL Server creates the database.

16 To close the SQL Server window, choose **Close** from its Server menu.

17 To close the TME Desktop window, choose **Close** from its Desktop menu.

18 Confirm the exit by clicking **Yes** in the confirmation dialog box.

19 At the UNIX prompt for the SQL server, type **exit**, then press **Return**.

- You are logged out and disconnected from the Tivoli Server.

Table 4.1-4 Creating User Database - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	**telnet** *TivoliServerName* **-or-** **rsh** *TivoliServerName*	**press Return**
2	*YourUserID* **-or-** (No entry)	**press Return -or-** (No action)
3	*YourPassword*	**press Return**

4	**setenv DISPLAY** *IPNumber*:**0.0 -or-** **setenv DISPLAY** *TivoliServerName*:**0.0**	**press Return**
5	**tivoli**	**press Return**
6	**Double-click the SQL Server icon**	(No action)
7	**Database Menu → Create**	**press Return**
8	**Name of database**	(No action)
9	**Database owner**	(No action)
10	**If for restore, check For Load**	(No action)
	For each database device allocation, steps 11-14:	
11	**Name of device**	(No action)
12	**Size of allocation**	(No action)
13	**For Log, click Log**	(No action)
14	**Click Add button**	(No action)
15	**Click OK**	(No action)
16	**SQL Server→Close**	**press Return**
17	**TME Desktop→Close**	**press Return**
18	**Click Yes**	(No action)
19	**exit**	**press Return**

4.1.3.3 Creating Segments

Database Segments are created when a database is created, when the Database Administrator determines that it is necessary to allocate database objects to a new or additional devices, or as part of the Database Recovery Procedure.

The Activity Checklist table that follows provides an overview of the segment creation process. Column one (**Order**) shows the order in which tasks should be accomplished. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task. Column three (**Task**) provides a brief explanation of the task. Column four (**Section**) provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found. Column five (**Complete**?) is used as a checklist to keep track of which task steps have been completed.

Table 4.1-5 Creating Segments - Activity Checklist

Order	Role	Task	Section	Complete?
1	System Admin.	Determine Need for New Segment	(I) 4.1.3.3	
2	DBA	Create new segment	(P) 4.1.3.3	

In order to perform the procedure, the DBA must have obtained the following information:

a. Name of database

b. Database device exists

c. Space on the database allocated to the Database device

To create a database, the DBA must have the following TME administrator roles:

a. user (TME)

b. space (ESSM)

c. sa_role (SQL Server)

Table 4.1-6 presents the steps required to create segments in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below:

1 Log into a Tivoli Server by typing: **telnet TivoliServerName** or **rsh TivoliServerName**, then press **Return**.

2 If a **Login**: prompt appears, log in as yourself by typing: **YourUserID**, then press **Return**.

- A password prompt is displayed.

3 Enter **YourPassword**, then press **Return**.

- Remember that YourPassword is case sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.

4 Set display to current terminal by typing: **setenv DISPLAY IPNumber:0.0** or **setenv DISPLAY TivoliServerName:0.0**, then press **Return**.

5 Type **tivoli**. Press **return**.

- You will now be in the TME Desktop for Administrator (your name) window.

6 Double-click the **SQL Server** icon in the policy region window to open the SQL Server Window.

7 Double-click the **Database** icon in the SQL Server window to open the Database Window.

8 Double-click the **Segments Manager** icon in the Database window to open the Segments Manager Window.

9 From the **Segments** menu of the SQL Server Window, choose **Create**.

- The Create Segment dialog box opens. You can now specify the attributes of the new segment.

10 Enter the **segment name** in the Name edit box.

For each database device on which the segment may reside, perform steps 11-12:

11 Select a **device name** in the Available Devices list.

12 To **add** a device to the Devices list, click the **right** arrow button.
- or -
To **remove** a device from the Devices list, click the **left** arrow.

13 Click the **Create** button.
- SQL Server creates the segment.
- The Segment dialog box replaces the Create Segment dialog box.

14 When finished viewing the current device allocations, click **Done** to close the Segment dialog box.

15 To close the Segments Manager window, choose **Close** from its Segment menu.

16 To close the Database window, choose **Close** from its Database menu.

17 To close the SQL Server window, choose **Close** from its Server menu.

18 To close the TME Desktop window, choose **Close** from its Desktop menu.

19 Confirm the exit by clicking **Yes** in the confirmation dialog box.

20 At the UNIX prompt for the SQL server, type **exit**, then press **Return**.
- You are logged out and disconnected from the Tivoli Server.

Table 4.1-6 Create Segment - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	**telnet** *TivoliServerName* **-or-** **rsh** *TivoliServerName*	**press Return**
2	*YourUserID* **-or-** (No entry)	**press Return -or-** (No action)
3	*YourPassword*	**press Return**
4	**setenv DISPLAY** *IPNumber*:**0.0 -or-** **setenv DISPLAY** *TivoliServerName*:**0.0**	**press Return**
5	**tivoli**	**press Return**
6	**Double-click the SQL Server icon**	(No action)
7	**Double-click the Database icon**	(No action)
8	**Double-click the Segments Manager icon**	(No action)
9	**Segments Menu → Create**	**press Return**
10	**Name of Segment**	(No action)
	For each segment to allocate, steps 11-12:	

11	**Select device name**	(No action)
12	**Right arrow to add -or- left arrow to delete**	(No action)
13	**Click Create**	(No action)
14	**Click Done**	(No action)
15	**Segment→Close**	**press Return**
16	**Database→Close**	**press Return**
17	**SQL Server→Close**	**press Return**
18	**TME Desktop→Close**	**press Return**
19	**Click Yes**	(No action)
20	**exit**	**press Return**

4.1.3.4 Creating Dump Devices

A dump device is created when the System Administrator determines that a new device is available for use in dumping a Sybase database, in the Database Backup/Recovery Procedures. The System Administrator makes a request to the DBA who creates the new dump device and notifies the System Administrator when the device has been created.

The Activity Checklist table that follows provides an overview of the dump device creation process. Column one (**Order**) shows the order in which tasks should be accomplished. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task. Column three (**Task**) provides a brief explanation of the task. Column four (**Section**) provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found. Column five (**Complete**?) is used as a checklist to keep track of which task steps have been completed.

Table 4.1-7 Creating Dump Devices - Activity Checklist

Order	Role	Task	Section	Complete?
1	System Admin.	Confirm Need for a New Dump Device	(I) 4.1.3.4	
2	System Admin.	Request Creation of Dump Device by DBA	(I) 4.1.3.4	
3	DBA	Create New Dump Device	(P) 4.1.3.4	
4	DBA	Notify Requester and System Admin. when Dump Device is Available	(I) 4.1.3.4	

In order to perform the procedure, the DBA must have obtained the following information:

a. Name of dump device to create.

b. Physical device on which to place dump device.

To create dump devices, the DBA must have the following TME administrator roles:

a. user (TME)

b. space (ESSM)

c. sa_role (SQL Server)

Table 4.1-8 presents the steps required to create a dump device in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below:

1 Log into a Tivoli Server by typing: **telnet TivoliServerName** or **rsh TivoliServerName**, then press **Return**.

2 If a Login: prompt appears, log in as yourself by typing: **YourUserID**, then press **Return**.

- A password prompt is displayed.

3 Enter **YourPassword**, then press **Return**.

- Remember that YourPassword is case sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.

4 Set display to current terminal by typing: **setenv DISPLAY IPNumber:0.0** or **setenv DISPLAY TivoliServerName:0.0**, then press **Return**.

5 Type **tivoli**. Press **return**.

- You will now be in the TME Desktop for Administrator (your name) window.

6 Double-click the **SQL Server** icon in the policy region window to open the SQL Server Window.

7 Double-click the **Dump Devices Manager** icon in the SQL Server window to open the Dump Devices Manager window.

For each dump device to be created, do steps 8 through 13:

8 From the **Device** menu of the Dump Devices Manager window, choose **Create**.

- The Create Dump Device dialog box opens. You can now specify the attributes of the new dump device.

9 For **Logical Name**, enter the name you want to assign to the device.

10 For **Physical Name**, enter the full path name of the physical device in your environment to which to map the logical name.

11 Specify whether the dump device is a disk or tape device by selecting the **Disk** or **Tape** option button.

12 If the device is a tape device, enter its capacity in the **Size (MB)** box, in megabytes. This box is visible only if you select the Tape option button.

13 Click **Create**.

- SQL Server creates the dump device.

14 To close the **Dump Devices Manager** window, choose **Close** from its Device menu.

15 To close the **SQL Server** window, choose **Close** from its Server menu.

16 To close the **TME Desktop** window, choose **Close** from its Desktop menu.

17 Confirm the exit by clicking **Yes** in the confirmation dialog box.

18 At the **UNIX prompt** for the SQL server, type **exit**, then press **Return**.

- You are logged out and disconnected from the Tivoli Server.

Table 4.1-8 Creating Dump Devices - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	**telnet** *TivoliServerName* **-or-** **rsh** *TivoliServerName*	**press Return**
2	*YourUserID* **-or-** (No entry)	**press Return -or-** (No action)
3	*YourPassword*	**press Return**
4	**setenv DISPLAY** *IPNumber***:0.0 -or-** **setenv DISPLAY** *TivoliServerName***:0.0**	**press Return**
5	**tivoli**	**press Return**
6	**Double-click the SQL Server icon**	(No action)
7	**Double-click the dump devices icon**	(No action)
	For each dump device, steps 8-13	
8	**Device Menu → Create**	**press Return**
9	**Name of device**	(No action)
10	**Physical device**	(No action)
11	**Disk -or- Tape**	(No action)
12	**If tape, Device Size**	(No action)
13	**Click Create**	(No action)
14	**Dump Devices Manager→Close**	**press Return**
15	**SQL Server→Close**	**press Return**
16	**TME Desktop→Close**	**press Return**
17	**Click Yes**	(No action)
18	**exit**	**press Return**

4.1.4 Monitoring and Managing Resource Utilization

4.1.4.1 Use of Available Disk Space, Memory, Connection Error Logs, State of Transaction Logs, Device Problems, etc.

4.2 SQL Server Life Cycle Maintenance

The Activity Checklist table that follows provides an overview of SQL Server Life Cycle Maintenance process. Column one (**Order**) shows the order in which tasks should be accomplished. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task. Column three (**Task**) provides a brief explanation of the task. Column four (**Section)** provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found. Column five (**Complete?**) is used as a checklist to keep track of which task steps have been completed.

Table 4.2-1 SQL Server Life Cycle Maintenance - Activity Checklist

Order	Role	Task	Section	Complete?
1	DBA	Install the SQL Server Product	(I) 4.1.1	
2	DBA	Create a Managed SQL Server Resource	(P) 4.2.1	
3	DBA	Configure the SQL Server	(P) 4.2.2	
4	DBA	Start the SQL Server Resource	(P) 4.2.3	
5	DBA	Stop the SQL Server	(P) 4.2.4	

4.2.1 Create A Managed SQL Server Resource

A Managed SQL Server Resource is created when the Database Administrator determines that a new SQL server should be managed using the Enterprise SQL Server Manager (ESSM) product.

Detailed procedures for tasks performed by the DBA are provided in the sections that follow.

In order to perform the procedure, the DBA must have obtained the following information:

a. Name of the server to be managed.

b. Name of the host machine on which SQL Server is running.

c. Name of the host machine (TME client) on which ESSM management activities for the specified SQL Server are to occur**;** ESSM must be installed and running on the client.

To create an ESSM Managed SQL Server Resource, the DBA must have the following TME administrator roles:

a. user (TME)

b. server (at TMR level)

Table 4.2-2 presents the steps required to create a managed SQL server resource in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below:

1 Log into a Tivoli Server by typing: **telnet *TivoliServerName* or rsh TivoliServerName**, then press **Return**.

2 If a **Login:** prompt appears, log in as yourself by typing: ***YourUserID***, then press **Return**.

- A password prompt is displayed.

3 Enter ***YourPassword***, then press **Return.**

- Remember that ***YourPassword*** is case sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.

4 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0** or **setenv DISPLAY *TivoliServerName*:0.0**, then press **Return**.

5 Type **tivoli**. Press **Return.**

- You will now be in the TME Desktop for Administrator (your name) window.

6 Configure the policy region to allow SQL Server resources in the region.

7 Double-click the **policy region** icon in which you want the SQL Server Resource to reside..

8 Select **ManagedSQLServer** from the policy region **Create** menu.

- The Manage SQL Server dialog box is displayed.

9 Enter the **name of the SQL Server** to be registered as a managed resource in the box labeled **Name**.

10 Enter the **Name of the host machine** on which SQL Server is running in the box labeled **SQL Server Host.**

11 Enter the **Name of the host machine (TME client)** on which ESSM management activities for the specified SQL Server are to occur**.** in the box labeled **Management Host.**

12 Click the **OK** button to add the new SQL Server icon to the policy region.

13 To close the TME Desktop window, choose **Close** from its Desktop menu.

14 Confirm the exit by clicking **Yes** in the confirmation dialog box.

15 At the UNIX prompt for the machine to be backed up, type **exit**, then press **Return**.

- You are logged out and disconnected from the Tivoli Server.

Table 4.2-2 Create A Managed SQL Server Resource - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	**telnet** *TivoliServerName* **-or-** **rsh** *TivoliServerName*	**press Return**
2	*YourUserID* **-or-** (No entry)	**press Return -or-** (No action)
3	*YourPassword*	**press Return**
4	**setenv DISPLAY** *IPNumber*:**0.0 -or-** **setenv DISPLAY** *TivoliServerName*:**0.0**	**press Return**
5	**tivoli**	**press Return**
6		(No action)
7	**Double-click the Policy Region icon**	(No action)
8	**Create Menu → ManagedSQLServer**	**press Return**
9	**Enter SQL Server name**	(No action)
10	**Enter Name of SQL Server host**	(No action)
11	**Enter Name of Management host**	(No action)
12	**Click OK button**	**Click Proceed button**
13	**Desktop→Close**	**press Return**
14	**OK**	(No action)
15	**exit**	**press Return**

4.2.2 Configure SQL Server

A SQL Server is configured when the DBA determines that a customization or fine tuning is required to optimize memory allocation or performance.

In order to perform the procedure, the DBA must have obtained the following information:

a. Name of server to be configured

b. New values for configuration variables.

To set SQL server configuration variables, the DBA must have the following TME administrator roles:

a. user (TME)

b. server (ESSM)

c. sa_role (SQL Server)

d. The DBA must also have the **sso_role** (SQL Server) in order to set these SQL server configuration variables: **allow updates**, **audit queue size**, **password expiration interval**, or **remote access**.

Some parameter values take affect as soon as you reset the value. Others do not change until you reset the value and then reboot SQL Server. In the Server Configuration Parameters dialog box, parameters requiring a SQL Server reboot have a check mark in the Requires Restart column.

Table 4.2-3 presents the steps required to configure an SQL server in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below:

1 Log into a Tivoli Server by typing: **telnet *TivoliServerName* or rsh TivoliServerName**, then press **Return**.

2 If a **Login:** prompt appears, log in as yourself by typing: ***YourUserID***, then press **Return**.

- A password prompt is displayed.

3 Enter ***YourPassword***, then press **Return.**

- Remember that ***YourPassword*** is case sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.

4 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0** or **setenv DISPLAY *TivoliServerName*:0.0**, then press **Return**.

5 Type **tivoli**. Press **Return.**

- You will now be in the TME Desktop for Administrator (your name) window.

6 Double-click the **SQL Server** icon in the policy region window to open the SQL Server Window.

7 Select **Configuration** from the **Server** menu.

- The SQL Server Configuration dialog box opens and you are now able to view or set values for all SQL Server configuration variables.

For each parameter you want to update, repeat steps 8 through 10.

8 **Scroll** through the list of configuration parameters to locate one that you want to reset. Then, click anywhere in its row to select it.

- The name of the parameter you select appears above the NewValue group box.
- The Minimum and Maximum labels show the minimum and maximum allowed for a value.

9 Enter the **new value** of the configuration parameter in the edit box.

10 Click the **Change** button.

- SQL Server Manager updates the values of the New column to the values you entered.
- The New column shows the value most recently set for each configuration parameter.

11 Click **Apply**.

- SQL Server Manager updates the configuration values in the dialog box as follows and automatically issues a reconfigure command to SQL Server.
- If the parameter you reset takes affect immediately, SQL Server Manager copies the value in the New column to the Current column.
- If the parameter you reset requires an SQL Server reboot, SQL Server Manager does not update the Current column value until you reboot SQL Server. The Requires Restart column for such parameters contains a check mark.

12 To close the SQL Server Configuration window, click **Done**.

13 To close the TME Desktop window, choose **Close** from its Desktop menu.

14 Confirm the exit by clicking **Yes** in the confirmation dialog box.

15 At the UNIX prompt for the machine to be backed up, type **exit**, then press **Return**.

- You are logged out and disconnected from the Tivoli Server.

Table 4.2-3 Configure SQL Server - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	**telnet** *TivoliServerName* **-or-** **rsh** *TivoliServerName*	**press Return**
2	*YourUserID* **-or-** (No entry)	**press Return -or-** (No action)
3	*YourPassword*	**press Return**
4	**setenv DISPLAY** *IPNumber***:0.0 -or-** **setenv DISPLAY** *TivoliServerName***:0.0**	**press Return**
5	**tivoli**	**press Return**
6	**Double-click the SQL Server icon**	(No action)
7	**Server Menu → Configuration**	(No action)
	For each parameter to change, repeat steps 8-10	
8	**Scroll to parameter**	(No action)
9	**Enter new value**	(No action)
10	**Click Change button**	(No action)
11	**Click Apply button**	(No action)
12	**Click Done button**	(No action)
13	**Desktop→Close**	**press Return**
14	**Click Yes**	(No action)

15	exit	press Return

4.2.3 Start an SQL Server Process

An SQL server process is started when a new server is installed or after a system outage.

In order to perform the procedure, the DBA must have obtained the following information:

a. Database server name.

To start an SQL server process, the DBA must have the following TME administrator roles:

a. user (TME)

b. server (ESSM)

c. sa_role (SQL Server)

Table 4.2-4 presents the steps required to start an SQL server process in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below:

1 Log into a Tivoli Server by typing: **telnet TivoliServerName or rsh TivoliServerName**, then press **Return**.

2 If a **Login**: prompt appears, log in as yourself by typing: ***YourUserID***, then press **Return**.

- A password prompt is displayed.

3 Enter ***YourPassword***, then press **Return.**

- Remember that ***YourPassword*** is case sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.

4 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0** or **setenv DISPLAY *TivoliServerName*:0.0**, then press **Return**.

5 Type **tivoli**. Press **Return.**

- You will now be in the TME Desktop for Administrator (your name) window.

6 Double-click the **SQL Server** icon in the policy region window to open the SQL Server Window.

7 Select **Start** from the **Server** menu.

- The Start SQL Server dialog box opens and you are now able to start an SQL Server.

8 Enter the **RUN_*servername*_srvr** in the box labeled Runserver File Name.

9 Click the **OK** button.

- The SQL Server is started.

- The Start SQL Server dialog box closes.

10 To close the SQL Server window, choose **Close** from its Server menu.

11 To close the TME Desktop window, choose **Close** from its Desktop menu.

12 Confirm the exit by clicking **Yes** in the confirmation dialog box.

13 At the UNIX prompt for the machine to be backed up, type **exit**, then press **Return**.

Table 4.2-4 Start SQL Server - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	**telnet** *TivoliServerName* **-or-** **rsh** *TivoliServerName*	**press Return**
2	*YourUserID* **-or-** (No entry)	**press Return -or-** (No action)
3	*YourPassword*	**press Return**
4	**setenv DISPLAY** *IPNumber***:0.0 -or-** **setenv DISPLAY** *TivoliServerName***:0.0**	**press Return**
5	**tivoli**	**press Return**
6	**Double-click the SQL Server icon**	(No action)
7	**Server Menu → Start**	(No action)
8	**Enter RUN_*servername*_srvr**	(No action)
9	**Click OK button**	(No action)
10	**Server→Close**	**press Return**
11	**Desktop→Close**	**press Return**
12	**Click Yes**	(No action)
13	**exit**	**press Return**

4.2.4 Stop an SQL Server

An SQL server process is stopped when the system is going down for maintenance.

To stop an SQL server process, the DBA must have the following TME administrator roles:

a. user (TME)

b. server (ESSM)

c. sa_role (SQL Server)

Table 4.2-5 presents the steps required to stop an SQL server process in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below:

1 Log into a Tivoli Server by typing: **telnet *TivoliServerName* or rsh TivoliServerName**, then press **Return**.

2 If a **Login:** prompt appears, log in as yourself by typing: ***YourUserID***, then press **Return**.

- A password prompt is displayed.

3 Enter ***YourPassword***, then press **Return.**

- Remember that ***YourPassword*** is case sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.

4 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0** or **setenv DISPLAY *TivoliServerName*:0.0**, then press **Return**.

5 Type **tivoli**. Press **Return.**

- You will now be in the TME Desktop for Administrator (your name) window.

6 Double-click the **SQL Server** icon in the policy region window to open the SQL Server Window.

7 Select **Stop** from the **Server** menu.

- The Stop SQL Server dialog box opens and you are now able to stop a SQL Server.

8 For routine operation, select the **Wait for processes to end** button. For emergency shutdown select the **Stop immediately** button.

9 If required, select Restart server after shutdown.

10 Click the **OK** button.

- The SQL Server is stopped.
- If Restart server after shutdown was selected, the server is automatically restarted after shutdown..
- The Stop SQL Server dialog box closes.

11 To close the SQL Server window, choose **Close** from its Server menu.

12 To close the TME Desktop window, choose **Close** from its Desktop menu.

13 Confirm the exit by clicking **Yes** in the confirmation dialog box.

14 At the UNIX prompt for the machine to be backed up, type **exit**, then press **Return**.

Table 4.2-5 Stop an SQL Server - Quick-Step Procedures

Step	What to Enter or Select	Action to Take

1	**telnet** *TivoliServerName* **-or-** **rsh *TivoliServerName***	**press Return**
2	*YourUserID* **-or-** (No entry)	**press Return -or-** (No action)
3	*YourPassword*	**press Return**
4	**setenv DISPLAY** *IPNumber*:**0.0 -or-** **setenv DISPLAY** *TivoliServerName*:**0.0**	**press Return**
5	**tivoli**	**press Return**
6	**Double-click the SQL Server icon**	(No action)
7	**Server Menu → Stop**	(No action)
8	**Select Wait for processes to end -or- Stop immediately**	(No action)
9	**If required, select Restart server after shutdown**	
10	**Click OK button**	(No action)
11	**Server→Close**	**press Return**
12	**Desktop→Close**	**press Return**
13	**Click Yes**	(No action)
14	**exit**	**press Return**

4.3 SQL Server Logins and Privileges

Providing access to SQL servers and their databases consists of the following steps:

a. A server login account for a new user is created.

b. The user is added to a database and optionally assigned to a group.

c. The user or group is granted permissions on specific commands and database objects.

From time to time changes will be needed to user permissions for command and database objects.

The SQL Server Logins and Privileges processes begin when the requester fills out a "SQL Server Login Account Request Form" and submits it to his or her supervisor. The "SQL Server Login Account Request Form" includes information regarding the user (User Name, UNIX ID, Group, Organization, and Site) and databases to be accessed, permissions required for database objects, as well as the user's explanation of why a new login account or changes to an existing account on the SQL Server is needed. The requester's supervisor reviews the request, and if he or she determines that it is appropriate for the requester to obtain or change a SQL Server login account, forwards the request to the Operations Supervisor (Ops Super). The Ops Super verifies that all required information is contained on the form. (Incomplete forms are returned to the requester's supervisor for additional information.) If it is complete and if the request for a new or modified SQL Server login account fits within policy guidelines, the Ops Super approves the request and forwards the request form to the DBA to implement. After the user's login account is created, the DBA provides the user with a password to use for logging onto their SQL Server login. The user can change the initial password if local DAAC policy requires, or if he/she prefers to select his/her own password.

The DBA also sends an e-mail message to the user's supervisor informing him/her that the user's SQL Server login was created.

The Activity Checklist table that follows provides an overview of the SQL Server Login and Privileges process. Column one (**Order**) shows the order in which tasks should be accomplished. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task. Column three (**Task**) provides a brief explanation of the task. Column four (**Section**) provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found. Column five (**Complete?**) is used as a checklist to keep track of which task steps have been completed.

Table 4.3-1 SQL Server Login - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Complete SQL Server Login Form and Forward to Ops Supervisor	(I) 4.3	
2	Ops Super	Review Request and Forward to DBA	(I) 4.3	
3	DBA	Review and Forward to DAAC Mgr.	(I) 4.3	
4	DAAC Mgr	Approve/Deny Request in Accordance with Policy. Forward to DBA if approved.	(I) 4.3	
5	DBA	Create SQL Server Login	(P) 4.3.1	
6	DBA	Add User to One or More Databases	(P) 4.3.2	
7	DBA	Grant the User Permissions on Specific Commands and Database Objects	(P) 4.3. 3	
8	DBA	Modify the User Permissions on Specific Commands and Database Objects	(P) 4.3. 4	
9	DBA	Mail Password to User. Notify Supervisor and DAAC Mgr that login was Created.	(I) 4.3	

The procedures assume that the requester's application for an SQL Server login has already been approved by DAAC Management.

4.3.1 Creating SQL Server Login Accounts

In order to perform the procedure, the DBA must have obtained the following information:

a. User’s Operating System login name
b. User’s full name
c. Default password
d. Default database

To create a SQL Server login, the DBA must have the following TME administrator roles:

a. user (TME)
b. security (ESSM)
c. sso_role (SQL Server)

Table 4-3.2 presents the steps required to create an SQL Server login in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below:

1 Log into a Tivoli Server by typing: **telnet *TivoliServerName* or rsh TivoliServerName**, then press **Return**.

2 If a **Login:** prompt appears, log in as yourself by typing: ***YourUserID***, then press **Return**.

- A password prompt is displayed.

3 Enter ***YourPassword***, then press **Return.**

- Remember that ***YourPassword*** is case sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.

4 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0** or **setenv DISPLAY *TivoliServerName*:0.0**, then press **Return**.

5 Type **tivoli**. Press **Return.**

- You will now be in the TME Desktop for Administrator (your name) window.

6 Double-click the **SQL Server** icon in the policy region window to open the SQL Server Window.

7 Double-click the **Login Manager** icon in the SQL Server window to open the Logins Manager Window.

8 Select **Create** from the Login menu.

- The Create Login dialog box opens and you are now able to specify the attributes of the new login

9 Enter the **login name** for the new login in the box labeled **Name**.

10 Enter the **default password** for the new login in the box labeled **Password**.

11 Re-enter the **password** for the new login in the box labeled **Confirm**.

12 Enter the **User's full name** in the box labeled **Full Name**.

13 Enter the **default database** which the user will access in the box labeled **Database** within the **Defaults** Box.

14 If the user requires system administration roles,

- click on each of the required roles within the **Available Roles** box
- click on the **left arrow** button to add these roles to the **Selected Roles** box.

15 Click on the **Create** button to create the new login.

16 To close the SQL Server window, choose **Close** from its Server menu.

17 To close the TME Desktop window, choose **Close** from its Desktop menu.

18 Confirm the exit by clicking **Yes** in the confirmation dialog box.

19 At the UNIX prompt for the machine to be backed up, type **exit**, then press Return.

- You are logged out and disconnected from the Tivoli Server.

Table 4.3-2 Create SQL Server Login - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	**telnet** *TivoliServerName* **-or-** **rsh** *TivoliServerName*	**press Return**
2	*YourUserID* **-or-** (No entry)	**press Return -or-** (No action)
3	*YourPassword*	**press Return**
4	**setenv DISPLAY** *IPNumber*:**0.0 -or-** **setenv DISPLAY** *TivoliServerName*:**0.0**	**press Return**
5	**tivoli**	**press Return**
6	**Double-click the Login Manager icon**	(No action)
7	**Double-click the Database icon**	(No action)
8	**Login Menu → Create**	**press Return**
9	**Enter login name**	(No action)
10	**Enter default password**	(No action)
11	**Re-enter password**	(No action)
12	**Enter user's full name**	(No action)
13	**Enter default database**	(No action)
14	**If sys admin roles required, click each required role**	**Click left arrow button**
15	**Click Create button**	**Click Proceed button**
16	**Server→Close**	**press Return**
17	**Desktop→Close**	**press Return**
18	**OK**	(No action)
19	**exit**	**press Return**

4.3.2 Add User to Database(s)

In order to perform the procedure, the DBA must have obtained the following information:

a. User's SQL Server login name
b. User database name
c. Database to which user is added

To create a Database User, the DBA must have the following TME administrator roles:

a. user (TME)
b. security (ESSM)
c. sa_role (SQL Server)

Table 4.3-3 presents the steps required to add a user to a database in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below:

1 Log into a Tivoli Server by typing: **telnet *TivoliServerName*** or **rsh *TivoliServerName***, then press **Return**.

2 If a **Login:** prompt appears, log in as yourself by typing: ***YourUserID***, then press **Return**.

- A password prompt is displayed.

3 Enter ***YourPassword***, then press **Return.**

- Remember that ***YourPassword*** is case sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.

4 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0** or **setenv DISPLAY *TivoliServerName*:0.0**, then press **Return**.

5 Type **tivoli**. Press **Return.**

- You will now be in the TME Desktop for Administrator (your name) window.

6 Double-click the **SQL Server** icon in the policy region window to open the SQL Server Window.

7 Double-click the Database icon in the SQL Server window to open the Database Window.

8 Double-click the **Users Manager** icon in the **Database** window

- The **Users Manager** dialog box opens and you are now able to create a new user in the database

9 Select **Create** from the **User** menu.

- The Create User dialog box opens and you are now able to specify the attributes of the new user.

10 Enter the **name** for the new user in the box labeled **User**.

11 Select the requesters SQL Server Login from the scroll list labeled **Login**.

12 Click on the **Create** button to create the new user.

- The new user is created in the database.
- The Create User dialog box is replaced with the User Properties tab.

13 If required, you can, at this point, add the user to a group or add object or command permissions by following steps 11 through 21 in Section 4.3.3, below.

14 To close the Database window, choose **Close** from its Database menu.

15 To close the SQL Server window, choose **Close** from its Server menu.

16 To close the TME Desktop window, choose **Close** from its Desktop menu.

17 Confirm the **exit** by clicking Yes in the confirmation dialog box.

18 At the UNIX prompt for the Tivoli Server, type **exit**, then press **Return**.
You are logged out and disconnected from the Tivoli Server.

Table 4.3-3 Add User to a Database - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	**telnet** *TivoliServerName* **-or-** **rsh** *TivoliServerName*	**press Return**
2	*YourUserID* **-or-** (No entry)	**press Return -or-** (No action)
3	*YourPassword*	**press Return**
4	**setenv DISPLAY** *IPNumber*:**0.0 -or-** **setenv DISPLAY** *TivoliServerName*:**0.0**	**press Return**
5	**tivoli**	**press Return**
6	**Double-click the SQL Server icon**	(No action)
7	**Double-click the Database icon**	(No action)
8	**Double-click the Users Manager icon**	(No action)
9	**User Menu → Create**	**press Return**
10	**Enter name**	(No action)
11	**Select the SQL Server Login**	(No action)
12	**Click Create button**	(No action)
13	**If adding group or permissions, steps 11-21 of Table 4.3-4**	
14	**Database→Close**	**press Return**
15	**Server→Close**	**press Return**
16	**Desktop→Close**	**press Return**
17	**OK**	(No action)
18	**exit**	**press Return**

4.3.3 Granting Access Privileges

Granting access privileges consists of one or more of the following:

- Assigning a user to a group which has specific access privileges
- Assigning a user object permissions
- Assigning a user command permissions

In order to perform the procedure, the DBA must have obtained the following information:

User's SQL Server login name

a. User database name
b. Group to which user is to be assigned
c. Objects and specific permissions to assign
d. Commands and specific permissions to assign

To grant access privileges, the DBA must have the following TME administrator roles:

a. user (TME)
b. security (ESSM)
c. sa_role (SQL Server)

Table 4.3-4 presents the steps required to grant access privileges in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below:

1 Log into a Tivoli Server by typing: **telnet *TivoliServerName* or rsh *TivoliServerName***, then press **Return**.

2 If a **Login:** prompt appears, log in as yourself by typing: ***YourUserID***, then press **Return**.

- A password prompt is displayed.

3 Enter **YourPassword**, then press **Return.**

- Remember that ***YourPassword*** is case sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.

4 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0** or **setenv DISPLAY *TivoliServerName*:0.0**, then press **Return**.

5 Type **tivoli**. Press **Return.**

- You will now be in the TME Desktop for Administrator (your name) window.

6 Double-click the **SQL Server** icon in the policy region window to open the SQL Server Window.

7 Double-click the **Database** icon in the SQL Server window to open the Database Window.

8 Double-click the **Users Manager** icon in the **Database** window.

- The **Users Manager** dialog box opens and you are now able to create a new user in the database.

9 Select the **user** from the **Users Manager** window.

10 Choose **Properties** from the **User** menu.

- The User Properties tab of the User window opens and you are now able to specify the settings for the user.

If you are assigning the user to a group, perform step 11:

11 Select the **group name** from the pull–down list labeled **Group**.

- Click on the **Apply** button to assign the new group.

If you are granting permissions to database objects, repeat steps 12-17 as often as required to grant all permissions:

12 Click on the **Object Permissions** button

- The User Properties tab is replaced with the Object Permissions tab.

13 In the **Filter** box, click on the type of object for which permissions are to be granted: **Table**, **Procedure** or **View**.

14 In the **Permission Filter** box, click on **No Permissions**.

15 In the **Object** box, click on the object for which permissions are being granted.

16 In the box below the **Object** box, in the **Grant** row, click on the specific permissions to be granted. If the user should also be allowed to "grant permissions" to others, use the **With Grant** row instead of the **Grant** row.

17 Click on the **Apply** button to grant permissions.

If you are granting permissions to a command objects, follow steps 18 through 21.

18 Click on the **Command Permissions** button

- The User Properties or Object Permissions tab is replaced with the Command Permissions tab.

19 If permissions are to be granted for Database or Transaction Log Dump, click on the **Grant** button, in the **Dump** box, next to Database or Transaction, respectively.

20 If permissions are to be granted for other command(s), click on the **Grant** button, in the **Create** box, next to the corresponding command(s).

21 Click on the **Apply** button to grant permissions.

22 When all permissions have been granted, click on the **Done** button to close the permissions dialog.

23 To close the Users Manager window, choose **Close** from its User menu.

24 To close the Database window, choose **Close** from its Database menu.

25 To close the SQL Server window, choose **Close** from its Server menu.

26 To close the TME Desktop window, choose **Close** from its Desktop menu.

27 Confirm the exit by clicking **Yes** in the confirmation dialog box.

28 At the UNIX prompt for the Tivoli Server, type **exit**, then press **Return**.
You are logged out and disconnected from the Tivoli Server.

Table 4.3-4 Grant Access Privileges - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	**telnet** *TivoliServerName* **-or-** **rsh** *TivoliServerName*	**press Return**
2	*YourUserID* **-or-** (No entry)	**press Return -or-** (No action)
3	*YourPassword*	**press Return**
4	**setenv DISPLAY** *IPNumber*:**0.0 -or-** **setenv DISPLAY** *TivoliServerName*:**0.0**	**press Return**
5	**tivoli**	**press Return**
6	**Double-click the SQL Server icon**	(No action)
7	**Double-click the Database icon**	(No action)
8	**Double-click the Users Manager icon**	(No action)
9	**Double-click the user**	(No action)
10	**User Menu → Properties**	**press Return**
	If assigning user to a group, performs step 11	
11	**Group -> group name**	**click Apply**
	If granting permissions to database objects, repeat steps 12-17 as often as necessary	
12	**Click Object Permissions tab**	(No action)
13	**Click Table, Procedure or View**	(No action)
14	**Click No Permissions**	(No action)
15	**Click object of permissions**	(No action)
16	**Click specific permissions for Grant -or-WithGrant**	(No action)
17	**Click Apply button**	(No action)

	If granting permissions to command objects, follow steps 18-21:	
18	**Click Object Permissions tab**	(No action)
19	**If required, click Grant for Database or Transaction Dump**	(No action)
20	**Click Grant for each required Command**	(No action)
21	**Click Apply button**	(No action)
22	**Click Done button**	(No action)
23	**Users Manager→Close**	**press Return**
24	**Database→Close**	**press Return**
25	**SQL Server→Close**	**press Return**
26	**TME Desktop→Close**	**press Return**
27	**Click Yes**	(No action)
28	**exit**	**press Return**

4.3.4 Modifying Access Privileges

Modifying access privileges consists of one or more of the following:

- Changing the group to which a user has been assigned
- Granting additional object permissions or revoking existing object permissions
- Granting additional command permissions or revoking existing command permissions

In order to perform the procedure, the DBA must have obtained the following information:

a. User's SQL Server login name
b. User database name
c. New Group to which user is to be assigned
d. Objects and specific permissions to grant or revoke
e. Commands and specific permissions to grant or revoke

To grant or revoke access privileges, the DBA must have the following TME administrator roles:

a. user (TME)
b. security (ESSM)
c. sa_role (SQL Server)

Table 4.3-5 presents the steps required to grant or revoke access privileges in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below:

1 Log into a Tivoli Server by typing: **telnet *TivoliServerName* or rsh *TivoliServerName***, then press **Return**.

2 If a **Login:** prompt appears, log in as yourself by typing: ***YourUserID***, then press **Return**.

- A password prompt is displayed.

3 Enter ***YourPassword***, then press **Return.**

- Remember that ***YourPassword*** is case sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.

4 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0** or **setenv DISPLAY *TivoliServerName*:0.0**, then press **Return**.

5 Type **tivoli**. Press **Return.**

- You will now be in the TME Desktop for Administrator (your name) window.

6 Double-click the **SQL Server** icon in the policy region window to open the SQL Server Window.

7 Double-click the **Database** icon in the SQL Server window to open the Database Window.

8 Double-click the **Users Manager** icon in the **Database** window.

- The **Users Manager** dialog box opens and you are now able to create a new user in the database.

9 Select the **user** from the **Users Manager** window.

10 Choose **Properties** from the **User** menu.

- The User Properties tab of the User window opens and you are now able to specify the settings for the user.

If you are assigning the user to a group, perform step 11:

11 Select the new **group name** from the pull–down list labeled **Group**.

- Click on the **Apply** button to assign the new group.

If you are granting or revoking permissions to database objects, repeat steps 12-17 as often as required to grant all permissions:

12 Click on the **Object Permissions** button.

- The User Properties tab is replaced with the Object Permissions tab.

13 In the **Filter** box, click on the type of object for which permissions are to be granted or revoked: **Table**, **Procedure** or **View**.

14 In the **Permission Filter** box:

- Click on **No Permissions** to grant new permissions, **or**
- Click on **With Permissions** to revoke existing permissions

15 In the **Object** box, click on the object for which permissions are being granted or revoked.

16 In the box below the **Object** box,

- When granting permissions, click on the specific permissions to be granted in the **Grant** row. If the user should also be allowed to "grant permissions" to others, use the **With Grant** row instead of the **Grant** row.
- When revoking permissions, click on the specific permissions to be revoked in the **Revoke** row. If permissions which the user has granted to others should also be revoked, use the **With Cascade** row instead of the **Revoke** row.

17 Click on the **Apply** button to grant and/or revoke permissions.

If you are granting or revoking permissions to a command objects, follow steps 18-21:

18 Click on the **Command Permissions** button

- The User Properties or Object Permissions tab is replaced with the Command Permissions tab.

19 If permissions are to be granted or revoked for Database or Transaction Log Dump, click on the **Grant** or **Revoke** button, in the **Dump** box, next to Database or Transaction, respectively.

20 If permissions are to be granted or revoked for other command(s), click on the **Grant** or **Revoke** button, in the **Create** box, next to the corresponding command(s).

21 Click on the **Apply** button to grant and/or revoke permissions.

22 To close the Users Manager window, choose **Close** from its User menu.

23 To close the Database window, choose **Close** from its Database menu.

24 To close the SQL Server window, choose **Close** from its Server menu.

25 To close the TME Desktop window, choose **Close** from its Desktop menu.

26 Confirm the exit by clicking **Yes** in the confirmation dialog box.

27 At the UNIX prompt for the Tivoli Server, type **exit**, then press **Return**.
You are logged out and disconnected from the Tivoli Server.

Table 4.3-5 Modify Access Privileges - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	**telnet** *TivoliServerName* **-or-** **rsh** *TivoliServerName*	**press Return**
2	*YourUserID* **-or-** (No entry)	**press Return -or-** (No action)
3	*YourPassword*	**press Return**
4	**setenv DISPLAY** *IPNumber*:**0.0 -or-** **setenv DISPLAY** *TivoliServerName*:**0.0**	**press Return**

5	**tivoli**	**press Return**
6	**Double-click the SQL Server icon**	(No action)
7	**Double-click the Database icon**	(No action)
8	**Double-click the Users Manager icon**	(No action)
9	**Double-click the user**	(No action)
10	**User Menu → Properties**	**press Return**
	If changing group, performs step 11	
11	**Group -> group name**	**click Apply**
	If granting/revoking permissions to database objects, repeat steps 12-17 as often as necessary	
12	**Click Object Permissions tab**	(No action)
13	**Click Table, Procedure or View**	(No action)
14	**Click No Permissions or With Permissions**	(No action)
15	**Click object of permissions**	(No action)
16	**Click specific permissions for Grant -or- With Grant or Revoke -or- With Cascade**	(No action)
17	**Click Apply button**	(No action)
	If granting permissions to command objects, follow steps 18-21:	
18	**Click Command Permissions tab**	(No action)
19	**If required, click Grant or Revoke for Database or Transaction Dump**	(No action)
20	**Click Grant or Revoke for each required Command**	(No action)
21	**Click Apply button**	(No action)
22	**Users Manager→Close**	**press Return**
23	**Database→Close**	**press Return**
24	**SQL Server→Close**	**press Return**
25	**TME Desktop→Close**	**press Return**
26	**Click Yes**	(No action)
27	**exit**	**press Return**

4.4 Database Integrity

4.4.1 Checking Consistency

4.5 Backup and Recovery

4.5.1 Database and Transaction Log Backup

Non-scheduled database backups can be requested at any time by submitting a "Request for Database Backup Form" to the Ops Supervisor. The Ops Supervisor approves/denies the request.

When approved, the request is forwarded to the DBA who performs the backup and then notifies the requester and supervisor that the backup is complete.

A transaction log backup is performed as part of the database recovery process and consists of Task 3 in Table 4.5-1.

The Activity Checklist table that follows provides an overview of the database backup process. Column one (**Order**) shows the order in which tasks should be accomplished. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task. Column three (**Task**) provides a brief explanation of the task. Column four (**Section**) provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found. Column five (**Complete?**) is used as a checklist to keep track of which task steps have been completed.

Table 4.5-1 Database Backup - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Submit Request for Database Backup to Ops Supervisor	(I) 4.5.1	
2	Ops Super	Approve/Deny Request in Accordance with Policy. Forward to DBA if Approved.	(I) 4.5.1	
3	DBA	Perform Database Backup	(P) 4.5.1	
4	DBA	Notify Requester and Ops Super when Database Backup is Complete	(I) 4.5.1	

The procedures assume that the requester's application for a database backup has already been approved by DAAC Management. In order to perform the procedure, the DBA must have obtained the following information:

a. Name of database to be backed up

b. Name of the server on which the database resides

c. Name of the backup volume

d. Name of the dump file on the backup volume

To backup a database or transaction log, the DBA must have the following TME administrator roles:

a. user (TME)

b. dump (ESSM)

c. oper_role (SQL Server)

Table 4.5-2 presents the steps required to perform a database or transaction log backup in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

Note 1: If you run out of tapes at any time during this procedure, execute procedures in Section 3.2.5.2. "Labeling Tapes" of this document, and then return to this procedure.

1 Log into a Tivoli Server by typing: **telnet** ***TivoliServerName*** or **rsh** ***TivoliServerName***, then press **Return**.

2 If a **Login:** prompt appears, log in as yourself by typing: ***YourUserID***, then press **Return**.

- A password prompt is displayed.

3 Enter ***YourPassword***, then press **Return**.

- Remember that ***YourPassword*** is case sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.

4 Set display to current terminal by typing: setenv DISPLAY *IPNumber*:0.0 or setenv DISPLAY *TivoliServerName*:0.0, then press Return.

5 Type **tivoli**. Press **return.**

- You will now be in the TME Desktop for Administrator (your name) window.

6 Double-click the **SQL Server** icon in the policy region window to open the SQL Server Window.

7 Double-click the **Database** icon in the SQL Server window to open the Database Window.

8 Select **Backup** from the Database menu.

- The Backup Database dialog box opens and you are now able to perform a Database backup.

9 Click the **Database** or **Transaction Log** option in the upper left corner to specify whether to back up a database's data or its transaction log.

10 If backing up the transaction log, click **Backup, Truncate, and Log** to back up the transaction log, remove the inactive portion of the log, and create a new transaction log entry recording the backup

11 Click the **Name of a dump device** from the Dump Devices box.

12 Click the **OK** button to begin the backup.

13 If a volume change is required during the Backup Operation, a notice will be sent to the TME Administration notice group on the bulletin board.

14 To change a volume, double-click the database from the **SQL Server window** and choose **Change Volume** from the **Database menu**. The **Change Volume dialog box** opens.

15 **Type** the **Volume Name** and **File Name** for the new volume.

16 Mount the new tape and click the **Proceed** button to continue the Backup.

17 To close the Database window, choose **Close** from its **Database** menu.

18 To close the SQL Server window, choose **Close** from its **Server** menu.

19 To close the TME Desktop window, choose **Close** from its **Desktop** menu.

20 Confirm the exit by clicking **Yes** in the confirmation dialog box.

21 At the UNIX prompt for the SQL server, type **exit**, then press **Return**.

- You are logged out and disconnected from the Tivoli Server.

Table 4.5-2 Perform Database Backup - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	**telnet** *TivoliServerName* **-or-** **rsh** *TivoliServerName*	**press Return**
2	*YourUserID* **-or-** (No entry)	**press Return -or-** (No action)
3	*YourPassword*	**press Return**
4	**setenv DISPLAY** *IPNumber*:**0.0 -or-** **setenv DISPLAY** *TivoliServerName*:**0.0**	**press Return**
5	**tivoli**	**press Return**
6	**Double-click the SQL Server icon**	(No action)
7	**Double-click the Database icon**	(No action)
8	**Database Menu → Backup**	**press Return**
9	**Click the Database or Transaction Log button**	(No action)
10	**If transaction log, click Backup, Truncate, and Log**	(No action)
11	**Click the Name of a dump device**	(No action)
12	**Click the OK button**	(No action)
13	**Database menu → Change Volume**	**press Return**
14	**Type Volume Name**	(No action)
15	**Type File Name**	(No action)
16	**Mount the new tape**	**Click Proceed button**
17	**Database→Close**	**press Return**

18	Server→Close	press Return
19	Desktop→Close	press Return
20	Click Yes	(No action)
21	exit	press Return

4.5.2 Database Device Restore

A database recovery is performed when the System Administrator determines that a database device has failed. The System Administrator makes a request to the DBA, who performs the restore and notifies the System Administrator when the restore is complete.

The Activity Checklist table that follows provides an overview of the restore process. Column one (**Order**) shows the order in which tasks should be accomplished. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task. Column three (**Task**) provides a brief explanation of the task. Column four (**Section**) provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found. Column five (**Complete?**) is used as a checklist to keep track of which task steps have been completed.

Table 4.5.3 Database Device Restore - Activity Checklist

Order	Role	Task	Section	Complete?
1	System Admin.	Determine that Database Device Has Failed	(I) 4.5.2	
2	System Admin.	Request Restore by DBA	(I) 4.5.2	
3	DBA	Backup Transaction Log for Each Database on the Failed Device	(P) 4.5.1	
4	DBA	Examine Space Usage for Each Database on the Failed Device	(P) 4.5.2.1	
5	DBA	Delete Database(s) on Failed Device and the Failed Device	(P) 4.5.2.2	
6	DBA	Initialize New Device	(P) 4.1.3.1	
7	DBA	Re-create Each User Database	(P) 4.1.3.2	
8	DBA	Re-load Each Database from Database and Transaction Log Backups	(P) 4.5.2.3	
9	DBA	Notify Requester And System Admin. when Database Restore Is Complete	(I) 4.5.2	

The procedures assume that the device failure has been verified by the System Administrator. In order to perform the procedure, the DBA must have obtained the following information:

a. Name of database device which has failed

b. Name of replacement device

c. Name of the databases which reside on the failed device

d. Name of the backup volumes

e. Name of the dump files on the backup volumes

4.5.2.1 Examine Space Usage For Each Database on the Failed Device

4.5.2.2 Delete Database(s) on Failed Device and Delete the Failed Device

To delete a database(s) and/or devices, the DBA must have the following TME administrator roles:

a. user (TME)

b. space (ESSM)

c. sa_role (SQL Server)

Table 4.5-4 presents the steps required to delete a database on a failed device in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

To delete database(s) on failed device and the failed device, execute the procedure steps that follow:

1 Log into a Tivoli Server by typing: **telnet** ***TivoliServerName*** or **rsh** ***TivoliServerName***, then press **Return**.

2 If a **Login:** prompt appears, log in as yourself by typing: ***YourUserID***, then press **Return**.

- A password prompt is displayed.

3 Enter ***YourPassword***, then press **Return.**

- Remember that ***YourPassword*** is case sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.

4 Set display to current terminal by typing: **setenv DISPLAY** ***IPNumber*****:0.0** or **setenv DISPLAY** ***TivoliServerName*****:0.0**, then press **Return**.

5 Type **tivoli**. Press **return.**

- You will now be in the TME Desktop for Administrator (your name) window.

6 Double-click the **SQL Server** icon in the policy region window to open the SQL Server Window.

7 Double-click the **Database** icon in the SQL Server window to open the Database Window.

For each database on the failed device, do steps 8 through 10:

8 Click on the icon of the database to delete.

9 If the database is not damaged:

- Select **Delete** from the Database menu.

If the database is damaged

- Select **Delete Damaged** from the Database menu.

The Delete database confirmation dialog box is displayed.

10 Confirm the deletion by clicking **Yes** in the confirmation dialog box.

11 Back up the master database. See Section 4.5.1.

12 To close the Database window, choose **Close** from its **Database** menu.

13 Double-click the **database devices** icon in the SQL Server window to **open** the Database Devices Manager window.

14 Click on the icon of the device to delete.

15 Choose **Delete** from the Database Device menu.

- The Delete database device confirmation dialog box is displayed.

16 Confirm the deletion by clicking **Yes** in the confirmation dialog box.

17 To close the SQL Server window, choose **Close** from its **Server** menu.

18 To close the TME Desktop window, choose **Close** from its **Desktop** menu.

19 Confirm the exit by clicking **Yes** in the confirmation dialog box.

20 At the UNIX prompt for the SQL server, type **exit**, then press **Return**.

- You are logged out and disconnected from the Tivoli Server.

Table 4.5-4 Delete Database(s) on Failed Device and the Failed Device - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	**telnet** *TivoliServerName* **-or-** **rsh** *TivoliServerName*	**press Return**
2	*YourUserID* **-or-** (No entry)	**press Return -or-** (No action)
3	*YourPassword*	**press Return**
4	**setenv DISPLAY** ***IPNumber*****:0.0 -or-** **setenv DISPLAY** ***TivoliServerName*****:0.0**	**press Return**
5	**tivoli**	**press Return**
6	**Double-click the SQL Server icon**	(No action)
7	**Double-click the Database icon**	(No action)
8	**Click the database icon**	(No action)
9	**Database Menu → Delete -or- Delete Damaged**	**press Return**
10	**Click the Yes button**	(No action)
11	**Back up the master database (4.5.x)**	(No action)
12	**Database→Close**	**press Return**
13	**Double-click the database device icon**	(No action)
14	**Click device icon**	(No action)
15	**Database Device menu → Delete**	**press Return**
16	**Click the Yes button**	(No action)
17	**Server→Close**	**press Return**
18	**Desktop→Close**	**press Return**
19	**Click Yes**	(No action)
20	**exit**	**press Return**

4.5.2.3 Re-load Each Database from Database and Transaction Log Backups

To restore a Database and/or Transaction Log, the DBA must have the following TME administrator roles:

a. user (TME)

b. load (ESSM)

c. sa_role (SQL Server)

Table 4.5-5 presents the steps required to perform a database re-load in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below:

1 Log into a Tivoli Server by typing: **telnet** ***TivoliServerName*** or **rsh** ***TivoliServerName,*** then press **Return**.

2 If a **Login:** prompt appears, log in as yourself by typing: ***YourUserID***, then press **Return**.

- A password prompt is displayed.

3 Enter ***YourPassword***, then press **Return.**

- Remember that ***YourPassword*** is case sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.

4 Set display to current terminal by typing: **setenv DISPLAY** ***IPNumber*****:0.0** or **setenv DISPLAY** ***TivoliServerName*****:0.0**, then press **Return**.

5 Type **tivoli**. Press **return.**

- You will now be in the TME Desktop for Administrator (your name) window.

6 Double-click the **SQL Server** icon in the policy region window to open the SQL Server Window.

For each database which must be restored, restore the most recent backup. Then load each transaction log backup which was created since the database backup, in the sequence in which it was created. For the database backup restore and each of the transaction log loads, follow steps 7 through 25, below.

7 Double-click the **Database** icon in the SQL Server window to open the Database Window.

8 Select **The Database Options** from the Database menu.

- The Database Options dialog box opens
- You are now able to set the database options to prevent users from making changes from the time you begin restoring a database until the time you finish applying the last transaction log backup

9 Click the **checkbox** for the following options:

- Single-User Mode
- No Checkpoint On Recovery
- Read Only
- Usable by Database Owner Only

10 Click the OK button.

- SQL Server resets the options for the database.

11 Select **Restore...** from the Database menu.

- The Database Restore dialog box opens.

12 If you are restoring the database backup, select **Database** to specify restoring the database.

If you are restoring a transaction log, select **Transaction Log** to specify restoring from a transaction log backup.

13 In the **Dump File** edit box, enter the **file name** of the backup from which you are restoring.

14 If the dump device is a tape, enter the **volume name** in the **Tape Volume** edit box.

15 In the **Dump Devices** group box, specify the dump device or devices to use for the restoration. For each dump device, provide the following information:

- For **Name**, select the name of the physical or logical dump device from the drop-down list. Enter the **absolute pathname** for a physical device.
- For a remote Server, enter the **name** of the Backup Server for the SQL Server on which the database or transaction log resides.

16 To add a set of dump device specifications to the Database Devices list, click **Add**.

To delete an entry, highlight it and click **Remove**.

To change an entry, highlight it, make changes, and click **Change**.

17 Click the **OK** button to start the restore.

18 If a volume change is required during the Restore Operation, a notice will be sent to the TME Administration notice group on the bulletin board. To change a volume, open the database from the SQL Server window and choose Change Volume from the Database menu.

- The **Change Volume** dialog box opens.

19 Mount a new tape volume.

20 Optionally, enter the **name** of the new tape volume in the **Volume Name** box. Backup Server uses this name to confirm that the correct tape volume has been mounted. If you do not enter a name, Backup Server uses the name specified in the Tape Volume box of the Database Restore dialog box. If the Tape Volume box is blank, Backup Server does not check the ANSI tape label before continuing the restore.

21 Optionally, enter the **name** of the file to restore in the File to Restore box. If you do enter a name, Backup Server uses the name specified in the Dump File box of the Database Restore dialog box. If the Dump File box is blank, Backup Server restores the first file on the tape.

Note: If you enter a tape volume name in the Volume Name box, you must also enter a filename in the File to Restore box.

22 Click **Proceed**. Backup Server checks the tape and then continues the restore.

23 Select **The Database Options** from the Database menu.

- The Database Options dialog box opens
- You are now able to reset the database options to allow users to make changes to the database.

24 Click the **checkbox** for the following options:
- Single-User Mode
- No Checkpoint On Recovery
- Read Only
- Usable by Database Owner Only

25 Click the **OK** button.
- SQL Server resets the options for the database.

26 To close the Database window, choose **Close** from its **Database** menu.

27 To close the SQL Server window, choose **Close** from its **Server** menu.

28 To close the TME Desktop window, choose **Close** from its **Desktop** menu.

29 Confirm the exit by clicking **Yes** in the confirmation dialog box.

30 At the UNIX prompt for the Tivoli Server, type **exit**, then press **Return**.
- You are logged out and disconnected from the Tivoli Server.

Table 4.5-5 Re-load Databases from Database and Transaction Log Backups - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	**telnet** *TivoliServerName* **-or-** **rsh** *TivoliServerName*	**press Return**
2	*YourUserID* **-or-** (No entry)	**press Return -or-** (No action)
3	*YourPassword*	**press Return**
4	**setenv DISPLAY** *IPNumber*:**0.0 -or-** **setenv DISPLAY** *TivoliServerName*:**0.0**	**press Return**
5	**tivoli**	**press Return**
6	**Double-click the SQL Server icon**	(No action)
	For the database backup and each transaction log backup, repeat steps 7-25.	
7	**Double-click the Database icon**	(No action)
8	**Database Menu → Database Options**	**press Return**
9	**Click checkbox for options: Single-User Mode, No Checkpoint On Recovery, Read Only, and Usable by Database Owner Only**	(No action)
10	**Click the OK button**	(No action)
11	**Database menu → Restore**	**press Return**
12	**Select Database -or- Transaction Log**	(No action)

13	**Backup file name**	(No action)
14	**Tape volume name**	(No action)
15	**Dump Device Name -or- Backup Server Name**	(No action)
16	**Add -or- Remove -or- Change**	(No action)
17	**Click the OK button**	(No action)
	If volume change:	(No action)
18	**SQL server→Database→Change Volume**	**press Return**
19	**Mount tape**	(No action)
20	**Tape volume name**	(No action)
21	**File name**	(No action)
22	**Click Proceed**	(No action)
23	**Database Menu → Database Options**	**press Return**
24	**Click checkbox for options: Single-User Mode, No Checkpoint On Recovery, Read Only, and Usable by Database Owner Only**	(No action)
25	**Click the OK button**	(No action)
26	**Database→Close**	**press Return**
27	**Server→Close**	**press Return**
28	**Desktop→Close**	**press Return**
29	**Click Yes**	(No action)
30	**exit**	**press Return**

4.6 ECS DAAC-Configured Databases

4.6.1 Database Size Estimates and Planning

4.6.2 Database-unique Attributes

4.6.3 Database Reports

4.7 Database Tuning and Performance Monitoring

4.7.1 Design and Indexing

4.7.2 Queries

4.7.3 Monitoring and Boosting Performance

4.8 Troubleshooting

4.8.1 Diagnosing Database System Problems

4.8.1.1 Reports

4.8.1.2 Queries

4.8.2 On-call User Support and Emergency Response

5. Security Services

ECS security architecture must meet the requirements for data integrity, availability, and confidentiality. ECS Security Services meets these requirements by incorporating a variety of mechanisms to establish and verify user accounts, issue and verify passwords, audit user activity, and verify and protect data transfer. Security logs will be monitored and security reports generated by TO BE DETERMINED. Several COTS products provide tools for authentication and network and system monitoring: Kerberos, SATAN, Crack, npassword, TCP Wrapper, and Tripwire. The Open Software Foundation's Distributed Computing Environment (OSF/DCE) employs Kerberos for authenticating user requests for network services. (DCE administration tools are discussed in Section 3 of this document.) The COTS product, SATAN, monitors networks and finds system security vulnerabilities. Two COTS products — Crack and npassword — provide additional password protection for local system and network access. To monitor and control access to network services, ECS Security Services uses TCP Wrapper. The package, Tripwire, monitors changes to files and flags any unauthorized changes. Security Services also supports detection of, reporting, and recovery from security breaches. The products used for this tasking are TO BE DETERMINED.

This section defines step-by-step procedures for M&O personnel to run the Security Services tools. The procedures assume that the requester's application for a Security process has already been approved by DAAC Management. It is recommended that access to these tools be controlled through the **root access only**.

The Activity Checklist table that follows provides an overview of the Security process. Column one (**Order**) shows the order in which tasks are presented in this section. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task. Column three (**Task**) provides a brief explanation of the task. Column four (**Section)** provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found. Column five (**Complete?**) is used as a checklist to keep track of which task steps have been completed.

Table 5-1 Security - Activity Checklist

Order	Role	Task	Section	Complete ?
1	Super User	Run Security Log Analyst Program	(P) 5.1	
2	Super User	Generate Security Reports	(P) 5.2	
3	Super User	Run Network Authentication Service	(P) 5.3	
4	Super User	Monitor Network Vulnerabilities	(P) 5.4	
5	Super User	Ensure Password Integrity	(P) 5.5	
6	Super User	Monitor Requests for Network Services	(P) 5.6	
7	Super User	Monitor File and Directory Integrity	(P) 5.7	

8	Super User	Report Security Breaches	(P) 5.8	
9	Super User	Initiate Recovery from Security Breaches	(P) 5.9	

5.1 Generating Security Reports

All COTS security products generate reports and log files. These are available when you run the product. Your System Administrator will be able to assist you.

5.2 Running the Network Authentication Service

Because intruders can monitor network traffic to intercept passwords, traditional authentication methods are not suitable for use in computer networks. The use of strong authentication methods that prevent password disclosure is essential. The Kerberos Network Authentication Service is well suited for such an environment.

Developed at the Massachusetts Institute of Technology, Kerberos is a distributed authentication service that allows a client (process that makes use of a network service) running on behalf of a principal (user or server) to identify itself to other principals, without sending data across the network that might allow an intruder to subsequently impersonate the user. Not knowing the identity of a user who requests an operation makes it difficult to decide whether the operation should be permitted.

The principal's level of permissions (such as read, create, modify, destroy) is based on DCE permissions and passwords established for the user. Kerberos reinforces DCE password security through its use of DES encryption (secret key) to protect sensitive information on an open network. In the case of a human user as the principal, the secret key is based on the user's password. However, the principal's password is **never** passed through the network.

Kerberos authentication activities are transparent to the user. Communication is between servers (principals) and processes (clients). The principal's request must receive a "ticket" that will be passed to each network service that the principal wants to access. The ticket is a record that helps a client authenticate itself to a server; it contains the client's identity, a session key, a timestamp, and other information, all sealed using the server's secret key. The session key is a temporary encryption key used between two principals, with a lifetime limited to the duration of a single login "session" (usually 8 hours).

Several utility programs must be installed on the user's workstation to allow users to obtain Kerberos credentials (kinit), list credentials (klist), and destroy credentials (kdestroy).

These procedures assume that the site is running MIT Kerberos 5, that the System Administrator has logged in as a super user, and that the Kerberos Authentication Server is available.

1 To login to the Kerberos Service, type **/bin/kinit** then press [RETURN]**.**
Enter name and password.

- Acquires a ticket that is valid for the time of the session from the Kerberos authentication server. Once logged in, you will have access to the system as permitted by the tickets obtained from the Ticket Granting Service.

The following options can be used with the **kinit** command:

-f This option allows a ticket-granting ticket with a different network address than the present ticket-granting ticket's to be issued to the principal. For "forwarding" tickets to be granted, the principal's account in the registry must specify that the principal can be granted forwarding (or FORWARDABLE) tickets.

-v Specifies that the command should run in verbose mode.

2 At command line, type **klist** then press [RETURN].

- Acquires a list of tickets obtained for this session, for example:

```
Kerberos Ticket Information:
Ticket cache: /opt/dcelocal/var/security/creds/dcecred_031d6500
Default principal: reginald@edfcell.hitc.com
Server: krbtgt/edfcell.hitc.com@edfcell.hitc.com
        valid 96/09/09:10:36:16 to 96/09/09:20:36:16
Server: dce-rgy@edfcell.hitc.com
        valid 96/09/09:10:36:21 to 96/09/09:20:36:16
Server: dce-ptgt@edfcell.hitc.com
        valid 96/09/09:10:36:25 to 96/09/09:12:36:25
Client: dce-ptgt@edfcell.hitc.com      Server: krbtgt/edfcell.hitc.com@edfcell.
hitc.com
        valid 96/09/09:10:36:25 to 96/09/09:12:36:25
Client: dce-ptgt@edfcell.hitc.com      Server: dce-rgy@edfcell.hitc.com
        valid 96/09/09:10:36:25 to 96/09/09:12:36:25
```

The following options can be used with the **klist** command:

-e Includes expired tickets in the display. Without this option, only current tickets are displayed.

-f Displays option settings on the tickets. The options are:

D (postdatable)
dF (postdated) (forwardable)
f (forwarded)
I (initial)
i (invalid)
P (proxiable)
p (proxy)
R (renewable)

3 To logout of Kerberos Service, type **/bin/kdestroy** then press [RETURN].

- Destroys the ticket when the user logs out.

To share and mount files with Kerberos authentication:

4 Type **share -F nfs -o kerberos /filesystem** then press [RETURN].

- Shares a file system with Kerberos authentication.

5 Type **mount -F nfs -o kerberos server:resource mountpoint** then press [RETURN].

- Mounts a file system with Kerberos authentication.

6 To check the Kerberos Authentication Server, type **/Kerberos/Kerberos.log**.

5.4 Monitoring Network Vulnerabilities

The Security Administrator Tool for Analyzing Networks (SATAN) is a testing and reporting tool that collects a variety of information about networked hosts. SATAN gathers information about specified hosts and networks by examining network services (for example, finger, NFS, NIS, ftp). SATAN also gathers general network information (network topology, network services run, types of hardware and software being used on the network). The data is used to point out system vulnerabilities. Data can be reported in a summary format. Problems are described briefly and pointers provided to patches or workarounds.

Periodically, the operator will run SATAN as **root**. The procedures are provided below.

1 Make sure that **DISPLAY** is set on your workstation. **Note:** SATAN is run only on the SMC side (msss5hp).

2 From **/usr/ecs/Rel_A/COTS/secmgmt/satan-1.1.1** type **./satan**.

3 From the **SATAN Control Panel**, select **SATAN Configuration Management**. Set all variables or use the default values.

4 **Go back** to the **SATAN Control Panel**.

5 From the **SATAN Control Panel**, select **SATAN Data Management**. Create the SATAN database if it does not exist. When you create the database for the first time, you will see a warning message concerning password disclosures. Take no action and continue. The database is stored as **satan-data** in the directory **/satan-1.1.1/results**.

6 You will be notified when the SATAN finishes creating the database and scans the system (network or cluster) for vulnerabilities.

7 From this screen, you can click on "Continue with Reporting and Analysis" or you can return to the **SATAN Control Panel**, to make this selection. Select the reports that you want to review.

5.5 Ensuring Password Integrity

One aspect of system security is discretionary access control based on user passwords. Passwords should be so unique that they are virtually impenetrable to unauthorized users. Two COTS products provide utilities to create effective password practices. "Crack" detects weak passwords that could be easily bypassed, and "npasswd" enforces strong password rules.

Both of these products provide comprehensive dictionaries, which Crack and npasswd can shared. These "source" dictionaries provide lists of words, which if used, would create vulnerable passwords. You can add other dictionaries, for example, acronym lists, to eliminate commonly used terms from being used as passwords.

Crack and npasswd are installed in a secure location, that is, **root access only**. Such precautions are particularly apt when running Crack, which gives the administrator access to everyone's password that he/she penetrates.

5.5.1 Detecting Weak Passwords

Running Crack against a system's password file will enable a system administrator to assess how vulnerable the file is to unauthorized users and how well authorized users select secure passwords. Crack is designed to find standard Unix eight-character DES-encrypted passwords by standard guessing techniques.

Crack takes as its input a series of password files and source dictionaries. It merges the dictionaries, turns the password files into a sorted list, and generates lists of possible passwords from the merged dictionary or from information gleaned about users from the password file. It does not attempt to remedy the problem of allowing users to have guessable passwords, and it should NOT be used in place of getting a really good, secure password program replacement.

The instructions provided in the following sections are general in nature because how you configure Crack and how you run it depends on the platforms on which it resides and on the local security requirements established for your site. M&O personnel should be familiar with these tasks to:

1. Configure the Crack shellscript and config.h files based on the README file and on requirements established for your site. See Section 5.6.1.1, below.
2. Run Crack based on requirements established for your site. See Section 5.6.1.2, below.
3. Customize the dictionaries. See Section 5.6.1.3, below.

5.5.1.1 Configuring Crack

Although Crack should already be configured for your system, the instructions are provided should you have to reconstruct the makefile as a result of file corruption. Crack has two configuration files: the Crack shellscript, which contains all the installation-specific configuration data, and the file Sources/conf.h, which contains configuration options specific to various binary platforms.

1 In the Crack shellscript, edit the CRACK_HOME variable to the correct value. This variable should be set to an absolute path name through which the directory containing Crack may be accessed on ALL machines on which Crack will be run. (Path names relative to username are acceptable as long as you have some sort of csh.)

There is a similar variable, CRACK_OUT, which specifies where Crack should put its output files — by default, this is the same as $CRACK_HOME.

2 Edit the file Sources/conf.h and establish which switches to enable. Each #define has a small note explaining its purpose. Portability of certain library functions, should not be a problem.

3 If using Crack -network (see Section 5.6.1.4, below), generate a Scripts/ **network.conf** file. This file contains a list of hostnames to rsh to, what their binary type is (useful when running a network Crack on several different architectures), an estimate of their relative power (take your slowest machine as unary, and measure all others relative to it), and a list of per-host flags to add to those specified on the Crack command line, when calling that host. There is an example of such a file provided in the Scripts directory.

4 To specify a more precise figure as to the relative power of your machines, play with the **command make** tests in the source code directory. This can provide you with the number of fcrypt()s that your machine can do per second, which is a number that you can plug into your **network.conf** as a measure of your machines' power (after rounding the value to an integer).

5.6.1.2 Running Crack

Crack is a self-installing program. Once the necessary configuration options for the Crack shellscript and config.h have been set, the executables are created via **make** by running the Crack shellscript.

Notes for Yellow Pages (NIS) Users:

To get Crack running from a YP password file, the simplest way is to generate a passwd format file by running:-

```
ypcat passwd > passwd.yp
```

and then running Crack on this file.

To launch Crack:

1 From **/usr/ecs/Rel_A/COTS/secmgmt/crack**, at the command line type: **./Crack**

2 For the single platform version:

```
./Crack [options] [bindir] /etc/passwd [...other passwd files]
```

3 For the network version:

```
./Crack -network [options] /etc/passwd [...other passwd files]
```

For a brief overview of the [options] available, see Section 5.6.1.4, below. Section 5.6.1.5 briefly describes several very useful scripts.

5.5.1.3 Creating Dictionaries

Crack works by making many individual passes over the password entries that you supply to it. Each pass generates password guesses based upon a sequence of rules, supplied to the program by the user. The rules are specified in a simplistic language in the files gecos.rules and dicts.rules, located in the Scripts directory (see Section 5.6.1.5, below).

Rules in Scripts/gecos.rules are applied to data generated by Crack from the pw_gecos and pw_gecos entries of the user's password entry. The entire set of rules in gecos.rules is applied to each of these words, which creates many more permutations and combinations, all of which are tested. After a pass has been made over the data based on gecos information, Crack makes further passes over the password data using successive rules from the Scripts/dicts.rules by loading the whole of Dicts/bigdict file into memory, with the rule being applied to each word from that file. This generates a resident dictionary, which is sorted and uniqued so as to prevent wasting time on repetition. After each pass is completed, the memory used by the resident dictionary is freed up, and re-used when the next dictionary is loaded.

Crack creates the Dicts/bigdict dictionary by merging, sorting, and uniq'ing the source dictionaries, which are to be found in the directory DictSrc and which may also be named in the Crack shellscript, via the $STDDICT variable. (The default value of $STDDICT is /usr/dict/words.)

The file DictSrc/bad_pws.dat is a dictionary which is meant to provide many of those common but non-dictionary passwords, such as 12345678 or qwerty.

To create your own dictionary:

1 Copy your dictionary into the DictSrc directory (use compress on it if you wish to save space; Crack will unpack it while generating the big dictionary).

2 Delete the contents of the Dicts directory by running Scripts/spotless. Your new dictionary will be merged in on the next run.

5.5.1.4 Options

-f Runs Crack in foreground mode, i.e., the password cracker is not backgrounded, and messages appear on stdout and stderr as you would expect. This option is only really useful for very small password files, or when you want to put a wrapper script around Crack.

Foreground mode is disabled if you try running Crack-network -f on the command line, because of the insensibility of rshing to several machines in turn, waiting for each one to finish before calling the next. For more information, read the section about Network Cracking without NFS/RFS in the README.NETWORK file.

-v Sets verbose mode, whereby Crack will print every guess it is trying on a per-user basis. This is a very quick way of flooding your filestore, but useful if you think something is going wrong.

-m Sends mail to any user whose password you crack by invoking Scripts/nastygram with their username as an argument. The reason for using the script is so that a degree of flexibility in the format of the mail message is supplied; i.e., you don't have to recompile code in order to change the message.

-nvalue Sets the process to be nice()ed to value, so, for example, the switch -n19 sets the Crack process to run at the lowest priority.

-network Throws Crack into network mode, in which it reads the Scripts/network.conf file, splits its input into chunks which are sized according to the power of the target machine, and calls rsh to run Crack on that machine. Options for Crack running on the target machine may be supplied on the command line (for example, verbose or recover mode), or in the network.conf file if they pertain to specific hosts (e.g., nice() values).

-r<pointfile>

This is only for use when running in recover mode. When a running Crack starts pass 2, it periodically saves its state in a pointfile, with a name of the form Runtime/P.* This file can be used to recover where you were should a host crash. Simply invoke Crack in exactly the same manner as the last time, with the addition of the **-r** switch (for example, **-rRuntime/Pfred12345**). Crack will startup and read the file, and jump to roughly where it left off. If you are cracking a very large password file, this can save a lot of time after a crash.

5.5.1.5 Crack Support Scripts

The Scripts directory contains a small number of support and utility scripts, some of which are designed to help Crack users check their progress. The most useful scripts are briefly described below.

Scripts/shadmrg

This is a small script for merging /etc/passwd and /etc/shadow on System V style shadow password systems. It produces the merged data to stdout, and will need redirecting into a file before Crack can work on it.

Scripts/plaster

This is a simple frontend to the Runtime/D* diefiles that each copy of the password cracker generates. Invoking Scripts/plaster will kill off all copies of the password cracker you are running, over the network or otherwise. Diefiles contain debugging information about the job, and are generated so that all the jobs on the entire network can be called quickly by invoking Scripts/plaster. Diefiles delete themselves after they have been run.

Scripts/status

This script rshes to each machine mentioned in the Scripts/network.conf file, and provides some information about processes and uptime on that machine. This is useful when you want to find out just how well your password crackers are getting on during a Crack -network.

Scripts/{clean,spotless}

These are really just frontends to a makefile. Invoking Scripts/clean tidies up the Crack home directory, and removes probably unwanted files, but leaves the pre-processed dictionary bigdict intact. Scripts/spotless does the same as Scripts/clean but obliterates bigdict and old output files, too, and compresses the feedback files into one.

Scripts/nastygram

This is the shellscript that is invoked by the password cracker to send mail to users who have guessable passwords, if the **-m** option is used. Edit it to suit your system.

Scripts/guess2fbk

This script takes your out* files as arguments and reformats the 'Guessed' lines into a slightly messy feedback file, suitable for storing with the others.

An occasion where this might be useful is when your cracker has guessed many peoples' passwords, and then died for some reason (a crash?) before writing out the guesses to a feedback file. Running Scripts/guess2fbk out* >> Runtime/F.new will save the work that has been done.

5.5.1.6 Checking the Log

Crack loads dictionaries directly into memory, sorts and uniques them, before attempting to use each of the words as a guess for each users' password. If Crack correctly guesses a password, it marks the user as done and does not waste further time on trying to break that user's password.

Once Crack has finished a dictionary pass, it sweeps the list of users looking for the passwords it has cracked. It stores the cracked passwords in both plain text and encrypted forms in a feedback file in the directory **Runtime**. Feedback files have names of the form **Runtime/F***. The purpose of this is so that when it is next invoked, Crack can recognize passwords that it has successfully cracked previously, and filter them from the input to the password cracker. This provides an instant list of crackable users who have not changed their passwords since the last time Crack was run. This list appears in a file with name **out*** in the **$CRACK_OUT** directory, or on **stdout**, if foreground mode (**-f**) is invoked (see Section 5.6.1.4, above).

Similarly, when a Crack run terminates normally, it writes out to the feedback file all encrypted passwords that it has NOT succeeded in cracking. Crack will then ignore all of these passwords next time you run it.

Obviously, this is not desirable if you frequently change your dictionaries or rules, and so there is a script provided, **Scripts/mrgfbk**, which sorts your feedback files, merges them into one, and optionally removes all traces of "uncrackable" passwords, so that your next Crack run can have a go at passwords it has not succeeded in breaking before.

mrgfbk is invoked automatically if you run **Scripts/spotless** (see Section 5.6.1.5, above).

5.5.2 Enforcing Strong Passwords

"npasswd" is a "drop-in" replacement for the normal Unix "passwd" command, which is transparent to the user. npasswd performs some simple length and character type tests on a proposed password and then checks it against the words in the dictionaries and rules specified in the configuration file. When the user changes his/her password (or inputs one for the first time), npasswd will check the password against the dictionaries and the rules. If it passes the check, the password is accepted. If the password fails, npasswd provides a message to the user, explains why the password fails, and asks the user to try again.

5.5.2.1 Configuring npasswd

Configure npasswd to establish the password rules for your site:

1 Edit the makefile, **'npasswd.conf'**. Choose the version of npasswd you want to be the default (based on the platform on which npasswd will reside) and retarget '**all**' in the Makefile to point to it. For example,

- For running under **SunOS 4.X** system, set **OPTIONS = -DSUNOS4**. If you are thinking about running Sun "Secure RPC," add **DSECURE_RPC** to OPTIONS

- For running under **System V**, set **OPTIONS = -DSYSV**
- To use syslog(3), include **-DSYSLOG** in OPTIONS
- To update the 4.3BSD hashed password database, include **'-DBSD4_3'** in OPTIONS.
- Change the lines for 'CF' and 'HF' to retarget the config and or help files.

2 Continue to edit **'npasswd.conf'** to reflect your preferences. We recommend the following values:

```
# dictionary  /path/to/dictionary      Description
# dictionary  /usr/dict/words                  Standard word list
# dictionary  /usr/dict/new_words   Additional word list
# dictionary  /etc/local_words                 Local names to avoid
```

Note: npasswd can use the same dictionaries as Crack.

```
# Don't allow single-case passwords
        singlecase          no

# Minimum password length
        minlength           8

# Maximum effective password length
        maxlength
```

(warns that you have exceeded the maximum number of characters. If you type in 10 characters and the maxlength is 6, npasswd will accept the first 6 characters you type in.)

```
#Don't forbid unprintable characters
        printonly           yes
```

Disallow the '@' character because of its incompatibility with HP/UX. See "Replace illegal character list," below. (**Note:** Disallow "@" even if you are not working on an HP/UX.)

```
# Replace illegal character list
        badchars "<string>"         For example:  badchars          "@"
```

Set a list of characters forbidden in passwords.
This form REPLACES the built-in illegal character list (see below).
Control characters may be specified by the '^X' convention.

```
# Add to illegal character list
# badchars          +"<string>"
```

Adds to the built-in illegal character list. Uncomment if you want to use it.

3 Edit **'npasswd.help'** to reflect the preferences chosen for the password checking plus add any other local administrative details.

5.5.2.2 Building npasswd

These instructions are provided should you have to rebuild npasswd because of file corruption.

1 Do a '**make**' to build the executables.

2 Become super-user and do '**make install**'.

3 If you built npasswd with **-DSYSLOG**, modify **/etc/syslog.conf** to log messages for facility **LOG_AUTH** level **LOG_INFO**. This gives you a record of password changes.

5.6 Monitoring Requests for Network Services

With TCP Wrapper, you can monitor and filter incoming requests for network services, such as SYSTAT, FINGER, FTP, TELNET, RLOGIN, RSH, EXEC, TFTP, and TALK.

TCP Wrapper provides small daemon wrapper programs that can be installed without any changes to existing software or to existing configuration files. The wrappers report the name of the client host and the name of the requested service; the wrappers do not exchange information with the client or server applications, and impose no overhead on the actual conversation between the client and server applications. The usual approach is to run one single daemon process that waits for all kinds of incoming network connections. Whenever a connection is established, this daemon runs the appropriate server program and goes back to sleep, waiting for other connections.

M&O personnel will monitor requests for these network services:

Client	**Server**	**Application**
telnet	telnetd	remote login
ftp	ftpd	file transfer
finger	fingerd	show users
rlogin	rlogind	remote login
TFTP	TFTPd	Triviac FTP

You will monitor the **syslog** file. To view syslog, at the command line type

more/var/log/syslog

Standard Unix commands can be added, such as vi, emacs, or lp -d:

more/var/log/syslog | lp -d [printer name]

The syslog file provides information concerning who tried to access the network service. TCP Wrapper blocks any request made by unauthorized users. TCP Wrapper can be configured to send a message to any administrator whose request is rejected.

5.7 Monitoring File and Directory Integrity

Tripwire is a tool that aids in the detection of unauthorized modification of files resident on Unix systems. Tripwire is automatically invoked at system startup. This utility checks file and directory integrity by comparing a designated set of files and directories against information stored in a previously generated database. Tripwire flags and logs any differences, including added or deleted entries. When run against system files regularly, Tripwire spots any changes in critical system files, records these changes into its database, and notifies system administrators of corrupted or tampered files so that they can take damage control measures quickly and effectively. With

Tripwire, system administrators can conclude with a high degree of certainty that a given set of files remain free of unauthorized modifications if Tripwire reports no changes.

> **Note:** Since system files should not change and users' files change constantly, Tripwire should be used to **monitor only system files**. The list of system files you want to monitor is stored in **./configs/tw.conf**. See Section 5.8.2, below.

Tripwire is configured to mail the system administrator any output that it generates. However, some files on your system may change during normal operation, and this necessitates updating the Tripwire database.

5.7.1 Updating the Tripwire Database

You can update your Tripwire database in two ways. The first method is interactive, where Tripwire prompts the user whether each changed entry should be updated to reflect the current state of the file, while the second method is a command-line driven mode where specific files/entries are specified at run-time.

5.7.1.1 Updating Tripwire Database in Interactive mode

Running Tripwire in Interactive mode is similar to the Integrity Checking mode. However, when a file or directory is encountered that has been added, deleted, or changed from what was recorded in the database, Tripwire asks the user whether the database entry should be updated.

For example, if Tripwire is run in Interactive mode and a file's timestamp changed, Tripwire will print out what it expected the file to look like, what it actually found, and then prompt the user whether the file should be updated. For example,

```
/etc/hosts equiv
    st_mtime: Wed May  5 15:30:37 1993      Wed May  5 15:24:09 1993
    st_ctime: Wed May  5 15:30:37 1993      Wed May  5 15:24:09 1993
---> File:  /etc/hosts equiv
---> Update entry?  [YN(y)nh?] y
```

You could answer yes or no, where a capital 'Y' or 'N' tells Tripwire use your answer for the rest of the files. (The 'h' and '?' choices give you help and descriptions of the various inode fields.)

While this mode may be the most convenient way of keeping your database up-to-date, it requires that the user be "at the keyboard." A more conventional command-line driven interface exists, and is described next.

5.7.1.2 Updating Tripwire Database in Database Update Mode

Tripwire supports incremental updates of its database on a per-file/directory or tw.config entry basis. Tripwire stores information in the database so it can associate any file in the database with the tw.config entry that generated it when the database was created.

Therefore, if a single file has changed, you can:

tripwire -update /etc/newly.installed.file

Or, if an entire set of files that made up an entry in the tw.config file changed, you can:

tripwire -update /usr/local/bin/Local_Package_Dir

In either case, Tripwire regenerates the database entries for every specified file. A backup of the old database is created in the **./databases** directory.

Tripwire can handle arbitrary numbers of arguments in Database Update mode.

The script **twdb_check.pl** script is an interim mechanism to ensure database consistency. Namely, when new entries are added to the tw.config file, database entries may no longer be associated with the proper entry number. The twdb_check.pl script analyzes the database, and remaps each database entry with its proper tw.config entry.

5.7.2 Configuring the tw.config file

Edit your **tw.config** file in the **./configs** directory, or whatever filename you defined for the Tripwire configuration file, and add all the directories that contain files that you want monitored. The format of the configuration file is described in its header and in the "man" page. Pay especially close attention to the select-flags and omit-lists, which can significantly reduce the amount of uninteresting output generated by Tripwire. For example, you will probably want to omit files like mount tables that are constantly changed by the operating system.

Run Tripwire with **tripwire -initialize**. This will create a file called **tw.db_[hostname]** in the directory you specified to hold your databases (where [hostname] will be replaced with your machine hostname).

Tripwire will detect changes made to files from this point on. You ***must*** be certain that the system on which you generate the initial database is clean; however, Tripwire cannot detect unauthorized modifications that have already been made. One way to do this would be to take the machine to single-user mode, reinstall all system binaries, and run Tripwire in initialization mode before returning to multi-user operation.

This database must be moved someplace where it cannot be modified. Because data from Tripwire is only as trustworthy as its database, choose this with care. It is recommended to place all the system databases on a read-only disk (you need to be able to change the disk to writeable during initialization and updates, however), or exporting it via read-only NFS from a "secure-server." (This pathname is hardcoded into Tripwire. Any time you change the pathname to the database repository, you must recompile Tripwire. This prevents a malicious intruder from spoofing Tripwire into giving a false "okay" message.)

We also recommend that you make a hardcopy printout of the database contents right away. In the event that you become suspicious of the integrity of the database, you will be able to manually compare information against this hardcopy.

Once you have your database set up, you can run Tripwire in Integrity Checking mode by typing **tripwire** on the command line from the directory in which Tripwire has been installed.

5.8 Reporting Security Breaches

TO BE SUPPLIED.

5.9 Initiating Recovery from Security Breaches

TO BE SUPPLIED.

6. Network Administration

6.1 HPOpenView Network Node Manager (NNM)

HP OpenView Network Node Manager (NNM) is a multivendor network management application for use in managing TCP/IP networks and network devices that support the Simple Network Management Protocol (SNMP). NNM is an HP OpenView SNMP-based application running under the HP OpenView Windows (OVW) graphical user interface.

The NNM product is a configuration, performance, and fault management application for multivendor TCP/IP (Transmission Control Protocol/Internet Protocol) networks. NNM enables you to:

Automatically discover the devices on the TCP/IP network and monitor the status of those devices.

Automatically draw the Internet Protocol (IP) topology maps based on discovered information. A map is a graphical and hierarchical representation of your network and its systems. Discovered devices are placed in appropriate segments, networks, or Internet based on the topology of the IP network.

Manage any vendor devices that support the Simple Network Management Protocol (SNMP). NNM can manage standard MIB objects, as well as Enterprise-specific Management Information Base (MIB) objects.

Include new Enterprise-specific MIBs into the NNM MIB. Once you have loaded the new MIB module on the management station, you can manage any of the MIB objects defined in that MIB module.

The Activity Checklist table that follows provides an basic overview of the NNM functions. Column one (**Order**) shows the order in which tasks should be accomplished. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task. Column three (**Task**) provides a brief explanation of the task. Column four (**Section**) provides the Procedure (P) section number of Instruction (I) section number where details for performing the task can be found. Column five (**Complete?**) is used as a checklist to keep track of which task steps have been completed.

Table 6.1-1 Network Administration - Activity Checklist

Order	Role	Task	Section	Complete ?
1	Net Admin.	Start Network Node Manager	(P) 6.1.1	
2	Net Admin.	Add a Network Object	(P) 6.1.2.1	

3	Net Admin.	Add a Segment Object	(P) 6.1.2.2	
4	Net Admin.	Add a Node Object	(P) 6.1.2.3	
5	Net Admin.	Add an IP Interface Object	(P) 6.1.2.4	
6	Net Admin.	View the Current Network and System Configuration	(P) 6.1.3	
7	Net Admin.	View Network Address Information	(P) 6.1.4	
8	Net Admin.	View How Traffic is Routed on a Network	(P) 6.1.5	
9	Net Admin.	View the Services Available on a Node	(P) 6.1.6	

Detail procedures for tasks performed by the Network Administrator are provided in the sections that follow. The procedures assume that the administrator is authorized and has proper access privileges to perform the tasks.

6.1.1 Starting Network Node Manager (NNM)

HP Open View Network Node Manager is a set of applications that are integrated with HP Open View Windows (OVW). To Start NNM, HP OpenView Windows must be activated first. Once activated, OVW will automatically start NNM. HP OpenView windows will also automatically start the applications that are installed and registered.

Table 6.1-2 presents the procedures to start NNM in a condensed manner for quick reference. If you are already familiar with the procedures, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below.

Prerequisites for this Task

The network management processes that work with OVW and NNM must be running. The network management processes consist of the following HP OpenView background processes: **ovwdb, trapd, ovtopmd, ovactiond, snmpCollect,** and **netmon**. You can check to see if these processes are running with **/usr/ov/bin/ovstatus** command.

These procedures explain how to start the HP OpenView Windows graphical user interface:

1 Type **ovstart** at the command prompt and **press Enter**.

- If the network management processes are not running, you can start them by executing the **$OV_BIN/ovstart** command.

2 Type **ovstatus** at the command prompt and **press Enter**.

- This command will check the status of the processes.

3 Type **x11start** at the command prompt and **press Enter**.

- This command will start the X Windows session.

4 Type **ovw** at the command prompt and **press Enter**.

- The **$OV_BIN** directory must be in your path, this command will start HP OpenView Windows.
- If the **$OV_BIN** directory is not in your path, type **$OV_BIN/ovw** to start HP OpenView Windows.

To exit NNM and all other integrated applications, you must exit OVW. You can exit OVW in **one** of the following ways:

5 Select **File: Exit** from the menu bar of any submap window or go to step number 6;

6 **Click** on the **Close** button on all open submap windows until a black submap window is displayed. When the black submap window is displayed, click on the **Close** button.

- The open map is saved, and all the submap windows and dialog boxes of the map are closed. OVW, all NNM applications, and all other integrated applications are closed.

Table 6.1-2 Starting NNM (Network Node Manager) - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	ovstart $OV_BIN/ovstart if network management processes are not running	press Enter
2	ovstatus	press Enter
3	x11start	press Enter
4	ovw $OV_BIN/ovw if $OV_BIN directory is not in the path	press Enter
	To exit Network Node Manager: (2 methods)	
5	Exit	File → Exit
6	Close button on all open submap windows	single-click on Close button

6.1.2 Creating Additional Objects

To complete the distribution of resources over the map to better match how your network is organized, you must first expand the lower levels of the network map by creating additional network, segment, and node objects. The following sections show how to add network, segment, node, and interface objects to the network map so that IP Map will manage them.

6.1.2.1 Adding a Network Object

Table 6.1-3 presents the procedures to add a network object to the network map in a condensed manner for quick reference. If you are already familiar with the procedures, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below.

Prerequisites for this Task

The map must be opened with read-write access.

1 Type **ovstart** at the command prompt and **press Enter**.

- If the network management processes are not running, you can start them by executing the **$OV_BIN/ovstart** command.

2 Type **ovstatus** at the command prompt and **press Enter**.

- This command will check the status of the processes.

3 Type **x11start** at the command prompt and **press Enter**.

- This command will start the X Windows session.

4 Type **ovw** at the command prompt and **press Enter**.

- The **$OV_BIN** directory must be in your path, this command will start HP OpenView Windows.
- If the **$OV_BIN** directory is not in your path, type **$OV_BIN/ovw** to start HP OpenView Windows.

5 Select **Edit: Add object**

6 From the **symbol palette, choose the desired symbol type for the network object by selecting the desired subclass and use button 2 to drag the symbol to the submap**. The **Add object** dialog box appears.

7 Enter a selection name for the object in the **Selection Name** field of the **Add Object** dialog box.

8 In the **Object Attributes** list, select **IP Map** and click **Set Object Attributes**. The **IP Map Set Attributes** dialog box for a network object appears.

9 Enter a **Network Name.**

10 Enter a **Network Address**.

11 Optionally, **Network Subnet Mask** can be entered.

12 Click **Verify** to check for valid entries.

13 Click on **OK** to close the **Set Attributes** dialog box.

14 Click on **OK** in the **Add Object** dialog box to complete the operation.

Table 6.1-3 Adding a Network Object - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	ovstart $OV_BIN/ovstart if network management processes are not running	press Enter
2	ovstatus	press Enter
3	x11start	press Enter
4	ovw $OV_BIN/ovw if $OV_BIN directory is not in the path	press Enter
5	Edit:	select with mouse
6	Select the desired symbol type	select with mouse
7	Selection Name	(No action)
8	Select IP Map	click Set Object Attributes
9	Enter Network Name	press Enter
10	Enter Network Address	press Enter
11	Enter Network Subnet Mask (Optional)	press Enter
12	Select Verify	select with mouse
13	Select OK to close the Set Attributes	select with mouse
14	Select OK in the Add Object	select with mouse

6.1.2.2 Adding a Segment Object

If it can identify which segment the node is on, IP Map places the segment on that node. If it cannot make the identification, IP Map places the segment on the default segment submap. The default segment submap is the submap created by IP Map when OVW was first started. If that submap has been deleted, the default segment submap becomes the oldest segment submap. IP Map discovers new nodes on segments attached to SNMP, IP addressable bridges and multi-port repeaters (hubs).

Table 6.1-4 presents the procedures to add a segment object to the network map in a condensed manner for quick reference. If you are already familiar with the procedures, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below.

Prerequisites for this Task

The map must be opened with read-write access.

1 Type **ovstart** at the command prompt and **press Enter**.

- If the network management processes are not running, you can start them by executing the **$OV_BIN/ovstart** command.

2 Type **ovstatus** at the command prompt and **press Enter**.

- This command will check the status of the processes.

3 Type **x11start** at the command prompt and **press Enter**.

- This command will start the X Windows session.

4 Type **ovw** at the command prompt and **press Enter**.

- The **$OV_BIN** directory must be in your path, this command will start HP OpenView Windows.
- If the **$OV_BIN** directory is not in your path, type **$OV_BIN/ovw** to start HP OpenView Windows.

5 Select **Edit: Add Object**.

6 From the **symbol palette, choose the desired symbol type for the segment object by selecting the desired class, then the desired subclass, and drag the symbol to the submap**. The **Add Object** dialog box appears.

7 Enter a selection name for the object in the **Selection Name** field of the **Add Object** dialog box.

8 In the **Object Attributes** list, select **IP Map** and click **Set Object Attributes**. The **IP Map Set Attributes** dialog box for a segment object appears. A figure of the dialog box follows this procedure.

9 Enter a **name for the segment**. It must be unique to other segment names in the submap.

10 Click **Verify** to check for valid entries.

11 Click on **OK** to close the **Set Attributes** dialog box.

12 Click on **OK** in the **Add Object** dialog box to complete the operation.

Table 6.1-4 Adding a Segment Object- Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	ovstart $OV_BIN/ovstart if network management processes are not running	press Enter
2	ovstatus	press Enter
3	x11start	press Enter
4	ovw $OV_BIN/ovw if $OV_BIN directory is not in the path	press Enter
5	Select Edit: Add Object	select with mouse
6	Desired symbol type for the segment object	select desired class,

	by	then the desired subclass, and drag the symbol to the submap
7	Enter Selection Name	press Enter
8	Select IP Map	click on Set Object Attributes
9	Enter a name for the segment (must be unique)	press Enter
10	Select Verify	select with mouse
11	Select OK to close the Set Attributes	select with mouse
12	Select OK in the Add Object dialog box	select with mouse

6.1.2.3 Adding a Node Object

An Object can be added that represents a node or a network device to Segment submap by placing one of the supported symbols on a Segment submap. Double-clicking on the node symbol opens a Node submap. IP Map discovers and manages the symbols that represent the Computer, Connector, and Net Device classes in a Node submap.

Table 6.1-5 presents the procedures to add a node object to the network map in a condensed manner for quick reference. If you are already familiar with the procedures, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below.

Prerequisites for this Task

The map must be opened with read-write access.

1 Type **ovstart** at the command prompt and **press Enter**.

- If the network management processes are not running, you can start them by executing the **$OV_BIN/ovstart** command.

2 Type **ovstatus** at the command prompt and **press Enter**.

- This command will check the status of the processes.

3 Type **x11start** at the command prompt and **press Enter**.

- This command will start the X Windows session.

4 Type **ovw** at the command prompt and **press Enter**.

- The **$OV_BIN** directory must be in your path, this command will start HP OpenView Windows.
- If the **$OV_BIN** directory is not in your path, type **$OV_BIN/ovw** to start HP OpenView Windows.

5 Select **Edit: Add Object**

6 From the **symbol palette, choose the desired symbol type for the node object by selecting the desired class, then the desired subclass, and drag the symbol to the submap**. The Add Object dialog box appears.

7 Enter a selection name for the object in the **Selection Name** field of the **Add Object** dialog box.

8 In the **Object Attributes** list, select **IP Map**, and click **Set Object Attributes**. The **IP Map Set Attributes** dialog box for a node object appears.

9 Enter the hostname of the node.

10 Enter the IP address of the node.

11 Click **Verify** to check for valid entries.

12 Click on **OK** to close the **Set Attributes** dialog box.

13 Click on **OK** in the **Add Object** dialog box to complete the operation.

Table 6.1-5 Adding a Node Object- Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	ovstart $OV_BIN/ovstart if network management processes are not running	press Enter
2	ovstatus	press Enter
3	x11start	press Enter
4	ovw $OV_BIN/ovw if $OV_BIN directory is not in the path	press Enter
5	Select Edit: Add Object	select with mouse
6	Desired symbol type for the segment object	select desired class, then the desired subclass, and drag the symbol to the submap
7	Enter selection name	press Enter
8	Select IP Map	click Set Object Attributes
9	Enter hostname of the node	press Enter
10	Enter the IP address of the node	press Enter
11	Select Verify	select with mouse
12	Select OK to close the Set Attributes	select with mouse
13	Select OK in the Add Object to complete the operation	select with mouse

6.1.2.4 Adding an IP Interface Object

IP interface can be added to a Node submap by placing an IP Interface symbol on a Node submap. This is done by entering the IP address of the interface.

Table 6.1-6 presents the procedures to add an IP interface object to the network map in a condensed manner for quick reference. If you are already familiar with the procedures, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below.

Prerequisites for this Task

The map must be opened with read-write access.

1 Type **ovstart** at the command prompt and **press Enter**.

- If the network management processes are not running, you can start them by executing the **$OV_BIN/ovstart** command.

2 Type **ovstatus** at the command prompt and **press Enter**.

- This command will check the status of the processes.

3 Type **x11start** at the command prompt and **press Enter**.

- This command will start the X Windows session.

4 Type **ovw** at the command prompt and **press Enter**.

- The **$OV_BIN** directory must be in your path, this command will start HP OpenView Windows.
- If the **$OV_BIN** directory is not in your path, type **$OV_BIN/ovw** to start HP OpenView Windows.

5 Select **Edit: Add Object**.

6 From the **symbol palette, select the IP Interface symbol in the Cards class**. The Add Object dialog box appears.

7 Enter a **selection name for the object in the Selection Name field of the Add Object dialog box**.

8 In the Object Attributes list, **select IP Map, and click Set Object Attributes**. The IP Map Set Attributes dialog box for an IP Interface object appears.

9 Enter the **IP Address for the IP interface**. The subnet mask is added for you.

10 Click **Verify** to check for valid entries.

11 Click on **OK** to close the Set Attributes dialog box.

12 Click on **OK** in the Add Object dialog box to complete the operation.

Table 6.1-6 Adding an IP Interface Object- Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	ovstart $OV_BIN/ovstart if network management processes are not running	press Enter
2	ovstatus	press Enter
3	x11start	press Enter
4	ovw $OV_BIN/ovw if $OV_BIN directory is not in the path	press Enter
5	Select Edit: Add Object	select with mouse
6	Select the IP Interface	select with mouse
7	Enter selection name for the object	press Enter
8	Select IP Map	select Set Object Attributes
9	Enter IP Address for the IP interface	press Enter
10	Select Verify	select with mouse
11	Select OK to close the Set Attributes dialog box	select with mouse
12	Select OK in the Add Object dialog box	select with mouse

6.1.3 Viewing the Current Network and System Configuration

NNM provides quick access to information about your network and system configurations. This section points you to the menu items available to accessing this information.

Table 6.1-7 presents the procedures to view the current network and system configuration in a condensed manner for quick reference. If you are already familiar with the procedures, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below.

Prerequisites for this Task

One or more nodes must be selected from the map. If you select more than one node, you receive a dialog box for each selected node.

1 Type **ovstart** at the command prompt and **press Enter**.

- If the network management processes are not running, you can start them by executing the **$OV_BIN/ovstart** command.

2 Type **ovstatus** at the command prompt and **press Enter**.

- This command will check the status of the processes.

3 Type **x11start** at the command prompt and **press Enter**.

- This command will start the X Windows session.

4 Type **ovw** at the command prompt and **press Enter**.

- The **$OV_BIN** directory must be in your path, this command will start HP OpenView Windows.
- If the **$OV_BIN** directory is not in your path, type **$OV_BIN/ovw** to start HP OpenView Windows.

5 Select the **object** for which you want a description.

6 Select Monitor: **Description - Selected Objects**. The **Object Description** dialog box appears.

7 In the **Object Description** dialog box, select **IP Map** and select **View/Modify Object Attributes**. The **Set Attributes** dialog box appears.

Table 6.1-7 Viewing the Current Network and System Configuration - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	ovstart $OV_BIN/ovstart if network management processes are not running	press Enter
2	ovstatus	press Enter
3	x11start	press Enter
4	ovw $OV_BIN/ovw if $OV_BIN directory is not in the path	press Enter
5	Select the object for which you want a description	select with mouse
6	Select Monitor: Description - Selected Object	select with mouse
7	Select IP Map	Select with mouse
7	Select View/Modify Object Attributes	Select with mouse

6.1.4 Viewing Network Address Information

This task is useful for determining the addresses associated with a node, without looking through configuration files. The information you see is real-time data taken from the node versus static information taken from a database.

Table 6.1-8 presents the procedures to view network address information in a condensed manner for quick reference. If you are already familiar with the procedures, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below.

Prerequisites for this Task

- The node must support SNMP.

- One or more SNMP nodes must be selected from the map. If you select more than one node, you receive a dialog box for each selected node.

1 Type **ovstart** at the command prompt and **press Enter**.
- If the network management processes are not running, you can start them by executing the **$OV_BIN/ovstart** command.

2 Type **ovstatus** at the command prompt and **press Enter**.
- This command will check the status of the processes.

3 Type **x11start** at the command prompt and **press Enter**.
- This command will start the X Windows session.

4 Type **ovw** at the command prompt and **press Enter**.
- The **$OV_BIN** directory must be in your path, this command will start HP OpenView Windows.
- If the **$OV_BIN** directory is not in your path, type **$OV_BIN/ovw** to start HP OpenView Windows.

5 Select a **node** on the map.

6 Use the **Monitor: Network Configuration - Addresses….** Operation to view the following information about each interface on the node:
- interface index
- interface name
- IP address
- network mask
- network address
- link-level address (physical address)

For example:

Index	Interface	IP address	Network Mask	Network Address	Link Address
4	lan1	126.1.0.2	255.255.0.0	126.1.0.0	0x01002033333
3	lan0	126.1.0.3	255.255.0.0	126.1.0.0	0x01000202222
2	lo0	222.0.0.1	255.0.0.0	222.0.0.0	<none>

Table 6.1-8 Viewing Network Address Information- Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	ovstart $OV_BIN/ovstart if network management processes are not running	press Enter
2	ovstatus	press Enter

3	x11start	press Enter
4	ovw $OV_BIN/ovw if $OV_BIN directory is not in the path	press Enter
5	Select a node on the map	select with mouse
6	Use the Monitor: Network Configuration - Addresses	select with mouse

6.1.5 Viewing How Traffic is Routed on a Network

This task lists the routing table information for a remote SNMP node. It can be useful in determining more efficient routes on the network, assessing the need for explicit routes and diagnosing connectivity problems. The information you see is real-time data taken from the node versus static information taken from a database.

Table 6.1-9 presents the procedures to view traffic routing in a condensed manner for quick reference. If you are already familiar with the procedures, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below.

When rerouting traffic on the network, there are two ways of performing the task:

- For temporary change, the command route command is used.
- For permanent change, netlinkrc needs to be edited and the system needs to be rebooted.

Prerequisites for this Task

- The node must support SNMP.
- One or more SNMP node must be selected from the map. If you select more than one node, you receive a dialog box for each selected node.

1 Type **ovstart** at the command prompt and **press Enter**.
- If the network management processes are not running, you can start them by executing the **$OV_BIN/ovstart** command.

2 Type **ovstatus** at the command prompt and **press Enter**.
- This command will check the status of the processes.

3 Type **x11start** at the command prompt and **press Enter**.
- This command will start the X Windows session.

4 Type **ovw** at the command prompt and **press Enter**.
- The **$OV_BIN** directory must be in your path, this command will start HP OpenView Windows.
- If the **$OV_BIN** directory is not in your path, type **$OV_BIN/ovw** to start HP OpenView Windows.

5 Select a **node** on the map.

6 Use the **Monitor: Network Configuration - Routing Table..** operation to view the following information about each destination node with which the selected node communications:

- destination name (default is a route that the system uses when it cannot find a specific route)
- name of the gateway (router) between the selected node and the destination
- type of route (for example, directly connected to a LAN, through a remote gateway, or route currently not available)
- network subnet mask associated with the route
- name of the interface that is used to reach the destination

Table 6.1-9 Viewing How Traffic is Routed on a Network- Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	ovstart $OV_BIN/ovstart if network management processes are not running	press Enter
2	ovstatus	press Enter
3	x11start	press Enter
4	ovw $OV_BIN/ovw if $OV_BIN directory is not in the path	press Enter
5	Select a node on the map	select with mouse
6	Select Monitor: Network Configuration - Routing Table	select with mouse

6.1.6 Viewing the Services Available on a Node

This task lists the IP networking services for which a remote SNMP node is listening. It is useful for determining what configured services a node is currently running. The information you see is real-time data taken from the node versus static information taken from the database.

Table 6.1-10 presents the procedures to view available services on a node in a condensed manner for quick reference. If you are already familiar with the procedures, you may prefer to use this quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below.

Prerequisites for this Task

- The node must support SNMP.
- One or more SNMP nodes must be selected from the map. If you select more than one node, you receive a dialog box for each selected node.

1 Type **ovstart** at the command prompt and **press Enter**.

- If the network management processes are not running, you can start them by executing the **$OV_BIN/ovstart** command.

2 Type **ovstatus** at the command prompt and **press Enter**.

- This command will check the status of the processes.

3 Type **x11start** at the command prompt and **press Enter**.

- This command will start the X Windows session.

4 Type **ovw** at the command prompt and **press Enter**.

- The **$OV_BIN** directory must be in your path, this command will start HP OpenView Windows.
- If the **$OV_BIN** directory is not in your path, type **$OV_BIN/ovw** to start HP OpenView Windows.

5 Select a **node** on the map.

6 Use the **Monitor: Network Configuration - Services**.. operation, to view the following information about the selected node:

- service protocol: either TCP (Transmission Control Protocol) or UDP (User Datagram Protocol).
- Port to which the service is bound.
- Service for which the node is listening (for example, telnet, nfs). If no service is listed, the service is either unavailable or unknown.

Table 6.1-10 Viewing the Services Available on a Node- Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	ovstart $OV_BIN/ovstart if network management processes are not running	press Enter
2	ovstatus	press Enter
3	x11start	press Enter
4	ovw $OV_BIN/ovw if $OV_BIN directory is not in the path	press Enter
5	Select a node on the map	select with mouse
6	Select Monitor: Network Configuration - Services	select with mouse

6.2 Diagnosing Network Problems

A fault within network is defined as something that causes those systems "to fail to meet their operational objectives." Three elements are involved in managing network faults: detection of the fault, isolation of the fault to a particular component, and correction of the fault. Fault management, therefore, may include the maintenance of error logs, error detection processes, and diagnostic testing procedures. For many managers, the term network management is synonymous with fault management.

Performance and fault management are difficult to separate. High performance usually implies a low incident of faults. Performance management, however, goes beyond minimizing faults; it is responsible for gathering statistics on the operation of the network, maintaining and analyzing logs of the state of the system, and optimizing network operation.

Sniffer Network Analyzer: Ethernet Monitor is used to make sure the network is working at its peak performance and will diagnose any possible fault within the network. The Ethernet Monitor is a network monitoring program. The monitor provides an accurate picture of network activity at any moment or a historical record on network activity over a period of time. This information helps you find traffic overloads, plan for network expansion, detect intruders, establish performance baselines, and distribute traffic more efficiently among servers and subnets.

The monitor's report capabilities let you communicate this information to others, complete with graphs and tables. The alarm capabilities alert you to problems with the network or with individual stations.

- This list summarizes the monitor's capabilities:
- Monitors up to 1,024 network stations
- Generates visible and audible alarms for the entire network or for individual stations
- Complies a historical alarm log
- Provides real-time traffic and historical information for individual stations and for the entire network
- Sorts statistics to show only the items that interest you
- Creates customized management reports
- Automatically prints selected information at set time intervals

Note: The Ethernet Monitor only monitors frames on the Ethernet network segment to which the Network Interface Card is attached.

7. System Monitoring

7.1 Checking the Health and Status of the Network

Once a network has been discovered by **HP Open View IP discovery and layout,** monitoring the state of the network can begin. Monitoring includes tasks, such as, checking the map for color alerts which indicate problems, creating submaps needing special monitoring, and checking for network changes.

Objects that have an abnormal condition can be identified without having to look at every object on the network map. A color alert on a symbol indicates that some part of that object may have problems. To isolate a fault somewhere on the network, follow the color alerts to increasingly more specific submaps until the specific object that is not functioning is reached. Follow color alerts by opening child submaps of objects that contain a color alert.

The Activity Checklist table that follows provides an overview of the monitoring process. Column one (**Order**) shows the order in which tasks should be accomplished. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task. Column three (**Task**) provides a brief explanation of the task. Column four (**Section)** provides the Procedure (P) number or Instruction (I) number where details for performing the task can be found. Column five (**Complete?**) is a checklist to keep track of which task steps have been completed.

Table 7.1-1 Monitoring - Activity Checklist

Order	Role	Task	Section	Complete?
1	Fault Manager	Starting NNM (Network Node Manger)	(P) 7.1.1	
1	Fault Manager	Verify that an object is not functioning	(P) 7.1.2	
2	Fault Manager	Looking at Maps for Color Alerts	(P) 7.1.3	
3	Fault Manager	Looking at Maps for New Nodes	(P) 7.1.4	
4	Fault Manager	Create Special Submaps for Monitoring Status	(P) 7.1.5	
5	Fault Manager	Checking for Event Notifications	(P) 7.1.6	
6	Fault Manager	Rediscovering Network	(P) 7.1.7	

Detailed procedures for tasks performed by the Fault Manger are provided in the sections that follow. The procedures assume the Network map is read-write, the IP map is enabled for the map, and is configured to display status. To interpret the meaning of status colors correctly, the

compound status scheme of the open map should be known. This tells how status propagates from objects in a submap to the parent object. The compound status scheme for the map from the **Map Description** dialog box can be identified by selecting **File: Describe/Modify Map.**

Section 7.1.1 explains how to start NNM(Network Node Manger). Section 7.1.2 explains how to verify that an object is not functioning. Section 7.1.3 explains how to look at maps for color alerts. Section 7.1.4 explains how to look at maps for new nodes. Section 7.1.5 explains how to create special submaps for monitoring status. Section 7.1.6 explains how to check for event notifications. Section 7.1.7 explains how to rediscover the Network.

If you are already familiar with the procedures, you may prefer to use the quick-step tables. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented in Sections 7.1.1 through 7.1.5

7.1.1 Starting NNM (Network Node Manager)

HP Open View Network Node Manager is a set of applications that are integrated with HP Open View Windows (OVW). To Start NNM, HP Openview Windows must be activated first. Once activated, OVW will automatically start NNM. HP Openview windows will also automatically start the applications that are installed and registered.

Prerequisites for this Task

The network management processes that work with OVW and NNM must be running. The network management processes consist of the following HP OpenView background processes: **ovwdb, trapd, ovtopmd, ovactiond, snmpCollect, and netmon**. You can check to see if these processes are running with **/usr/ov/bin/ovstatus** command.

This procedure explains how to start the HP OpenView Windows graphical user interface.

1 Type **$OV_BIN/ovstart** at the command prompt and **press enter**.
- If the network management processes are not running, you can start them by executing the **$OV_BIN/ovstart** command.

2 Type **ovstatus** at the command prompt and **press enter**.
- This command will check the status of the processes.

3 Type **x11start** at the command prompt and **press enter**.
- This command will start the X Windows session.

4 Type **$OV_BIN/ovw** at the command prompt and **press enter**.
- The **$OV_BIN** directory must be in your path, this command will start HP OpenView Windows.
- If the **$OV_BIN** directory is not in your path, type **$OV_BIN/ovw** to start HP OpenView Windows.

5 Type **ovw&** and **press enter**.
- OVW displays the About OVW dialog box. After a few moments, you see the OVW Windows

To exit NNM and all other integrated applications, you must exit OVW. You can exit OVW in one of the following ways:

6 Select **File: Exit** from the menu bar of any submap window or go to step number 7;

7 **Click** on the **Close** button on all open submap windows until a black submap window is displayed. When the black submap window is displayed, click on the **Close** button.
- The open map is saved, and all the submap windows and dialog boxes of the map are closed. OVW, all NNM applications, and all other integrated applications exit.

IMPORTANT: Do not use the quick step version of a procedure unless you are already very familiar with the procedure.

To start **NNM**, execute the steps provided in the table.

Table 7.1-1 Starting NNM - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	$OV_BIN/ovstart	press Return
2	ovstatus	press Return
3	x11start	press Return
4	$OV_BIN/ovw	press Return
5	ovw&	press Return

7.1.2 Verify That an Object Is Not Functioning

This section explains how to verify that an object is not functioning and assumes that HP Openview is running on the desktop. If not, then see section 7.1.1 To verify that an object is not functioning, any of the following procedures can be executed.

1 Select the **Monitor** pull down menu
2 Select **Device Configuration**
3 Select **System Information**

-or-

1 Select the **Diagnose** pull down menu
2 Select **Network Connectivity**
3 Select **Demand Poll**

-or-

1 Select the **Diagnose** pull down menu
2 Select **Network Connectivity**
3 Select **Ping**

If these operations do not produce any responses or they time out, then the node is probably down or otherwise unreachable over the network. See Section 7.1.5 Checking for Event Notifications to verify event status of the node. If a Fault has occured see Section 8 on Problem Management and Section 21 COTS Hardware Maintenance.

IMPORTANT: Do not use the quick step version of a procedure unless you are already very familiar with the procedure.

To verify that an object is not working, execute the steps provided in the table.

Table 7.1-1 Verify - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	Monitor	Use the pull down menu
2	Device Configuration	Pull down menu
3	System Information	Pull down menu

7.1.3 Looking at Maps for Color Alerts

This example assumes that HP Openview is running on the desktop. If not, then see section 7.1.1 In this example, the Root submap is displayed, and a yellow Internet symbol is displayed on the Root submap. Compound status for the open map is set to HP Open View Window Default.

1 **Double click** on the yellow **Internet** symbol
- The **Internet submap** opens and displays three IP networks attached to two gateways. One IP network symbol is yellow. This indicates a marginal problem with the network.

2 **Double click** on the yellow **IP network** symbol
- A **Network submap** opens and displays three segments attached to two gateways. One segment symbol is yellow. This indicates a problem somewhere on the segment.

3 **Double click** on the yellow **segment** symbol
- A **Segment submap** opens and displays the nodes attached to that segment. Of all the nodes in the segment, the workstation node is red. The problem is isolated to that workstation.

4 **Double click** on the red **workstation** symbol
- A **Node submap** opens and displays two interface symbols, which indicate that two interfaces are installed on the workstation. One of them is red.
- You have isolated the fault to a single card of a single node on your internet.

At this point see Section 8 on Problem Management and Section 21 COTS Hardware Maintenance.

IMPORTANT: Do not use the quick step version of a procedure unless you are already very familiar with the procedure.

To look at Maps for Color Alerts, execute the steps provided in the table.

Table 7.1-2 Color ALerts- Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	Internet Symbol	Double click
2	IP Network	Double click
3	Yellow segment symbol	Double click
4	Red workstation symbol	Double click

7.1.4 Looking at Maps for New Nodes

This section assumes that HP Openview is running on the desktop. If not, then see section 7.1.1 **IP Map** will automatically discover the **IP-addressable nodes** for the open map. The purpose of this section is to identify new objects that have been discovered and added to the open map. Because discovery is automated, additional symbols of objects on the network map will be seen. **IP Map** must be enabled for the map. This is the default. **IP Map** places new symbols directly on the submap if autolayout is enabled. IP Map places new symbols in the **New Object Holding Area** if autolayout is disabled for the submap.

1 To check the default **Segment submap** for any new nodes that may have been discovered, open the default **Segment submap** from the segment symbol in the Network submap.
- View the submap for any new symbols.

2 To easily see new symbols in the submap, disable autolayout for the submap. When autolayout is disabled, a **New Object Holding Area** appears at the bottom of the submap.
- All newly added symbols are placed in the **New Object Holding Area**.

7.1.5 Creating Special Submaps for Monitoring Status

This section assumes that HP Openview is running on the desktop. If not, then see section 7.1.1 Submaps can be created that are logically organized instead of physically organized. This will help to create logical submaps for specialized monitoring.

IMPORTANT: See section 4-5 of the **HP Openview Network Node Manager User's Guide** to use this feature.

7.1.6 Checking for Event Notifications

This section assumes that HP Openview is running on the desktop. If not, then see section 7.1.1 Anytime a change occurs on the network an event is generated. Through the **Network Node Manager's** internal processes, the event is sent to a predefined category in the **Events Browser** window. The **Events Categories** window provides a notification of when new events occur. This window has a button corresponding to each of the event categories. When the button that corresponds to a specific event category is clicked, a window listing the events for that specific category appears. These windows are **Event Browser** windows. When a button in the **Event Categories** window changes color, it is an indication that an event occurred on the network which relates to that category. The color of the button indicates the highest severity event in the category. The default categories included in the **Event Categories** window are:

Error Events. This indicates inconsistent or unexpected behavior.
Threshold Events. This indicates that a threshold was exceeded.
Status Events. This indicates an object or interface status changed to up or down, or an object or interface started or stopped responding to ICMP echo requests.
Configuration Events. This indicates a node's configuration changed.
Application Alert Events. This indicates an HP OpenView Window application generated an alarm or alert.
All Events. This list all the above events and other events in one dialog box.

In the following example the **Threshold Events** button is red, which indicates that a critical threshold was exceeded somewhere on the network.

1 Click on the **Threshold Events** button in the **Event Categories** window. The **Threshold Events Browser** dialog box appears with a chronological listing of the threshold events that have occurred, with the most recent events at the bottom of the list.
- Each event listed includes the severity, time the event occurred, node on which the event occurred, and a brief event message.

2 To view the node that generated the event shown in this example, select the event from the list and click on **Action → Highlight Source on Map.**
- A map will appear with the **busynode** node highlighted. At this point, select the highlighted node by clicking on it, and invoke appropriate operations from the menu bar to further diagnose and correct the situation which caused the threshold to be exceeded.

3 To delete the event, select the event and click on **Action → Delete → Selected Event.**
- This will delete only the selected event.

For more information about event notification, click on the **help** button in the dialog box for the event being viewed or select **View SNMP Events** from the **Help: Index → Task**

IMPORTANT: Do not use the quick step version of a procedure unless you are already very familiar with the procedure.

To check for **Event Notifications**, execute the steps provided in the table.

Table 7.1-6 Event Notifications - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	Threshold Events	press Return
2	Action	press Return
3	Highlight source on Map	press Return

7.1.7 Rediscovering the Network

This section assumes that HP Openview is running on the desktop. If not, then see section 7.1.1 Occasionally you may edit your maps beyond recognition and want to start from scratch.

1 Exit all Openview sessions (if running) **cd /usr/OV/bin** and then enter **ovstop** at the command line
- This will stop all HP OpenView processes

2 Remove the Openview database **(do a backup first)**
- **cd $OV_DB/openview**
- **rm -rf $OV_DB/openview/***

3 Remove all of the current events**.**
- **rm $OV_LOG/xnmevents.***
- **rm $OV_LOG/trapd.log***
- **rm $OV_LOG/netmon.trace***

4 Clear the SNMP cache**.**
- **cd /usr/OV/bin**
- **xnmsnmpconf -clearCache**

5 Re register OVW fields**.**
- **ovstart ovwdb**
- **ovw -fields**

6 Restart NNM**.**
- **ovstart**
- **ovw &**

IMPORTANT: Do not use the quick step version of a procedure unless you are already very familiar with the procedure.

Table 7.1-7 Rediscovery - Quick-Step Procedures

Step	What to Enter or Select	Action to Take

1	Stop all OVW sessions	select exit from pull down menu
2	ovstop	press enter
3	cd $OV_BIN/openview	press enter
4	rm -rf $OV_DB/openview/*	press enter
5	rm $OV_LOG/xnmevents.*	press enter
6	rm $OV_LOG/trapd.log*	press enter
7	rm $OV_LOG/netmon.trace*	press enter
8	xnmsnmpconf -clearCache	press enter
9	ovstart ovwdb	press enter
10	ovw -fields	press enter
11	ovstart	press enter
12	ovw &	press enter

7.2 Tivoli Enterprise Console

The Tivoli Enterprise Console (TEC) provides centralized processing and management of distributed events, the ability to allow shared or partitioned administrator responsiblities based on enterprise-defined areas of responsiblity, and a flexigble interface to view and respond to events based on the events severity, source, location, or other characteristics. The following tables document the Tivoli event configuration.

Table 7.2-1 Disk Event Configuration

Resource	Response Level	Trigger When	Threshold	Response
Inodes Free	Warning	Less than	200	Change icon.
	Severe	Less than	150	Send Tivoli notice. Change icon.
	Critical	Less than	100	Send Tivoli notice. Change icon. Popup alarm.
Inodes Used	Warning	Greater than	X	Change icon.
	Severe	Greater than	X	Send Tivoli notice. Change icon.
	Critical	Greater than	X	Send Tivoli notice. Change icon. Popup alarm.
% Inodes Used	Warning	Greater than	80	Change icon.
	Severe	Greater than	90	Send Tivoli notice. Change icon.
	Critical	Greater than	95	Send Tivoli notice. Change icon. Popup alarm.
Space Free	Warning	Less than	200 MB	Change icon.

	Severe	Less than	100 MB	Send Tivoli notice. Change icon.
	Critical	Less than	50 MB	Send Tivoli notice. Change icon. Popup alarm.
Space Used	Warning	Greater than	X	Change icon.
	Severe	Greater than	X	Send Tivoli notice. Change icon.
	Critical	Greater than	X	Send Tivoli notice. Change icon. Popup alarm.
% Space Used	Warning	Greater than	80	Change icon.
	Severe	Greater than	90	Send Tivoli notice. Change icon.
	Critical	Greater than	95	Send Tivoli notice. Change icon. Popup alarm.
Tivoli DB Free Space	Warning	Less than	20 MB	Change icon.
	Severe	Less than	10 MB	Send Tivoli notice. Change icon.
	Critical	Less than	5 MB	Send Tivoli notice. Change icon. Popup alarm.

Table 7.2-2 Security Event Configuration

Resource	**Response Level**	**Trigger When**	**Threshold**	**Response**
Check File Permission:				
/etc/passwd	Critical	Changes from	-rw-r--r--	Send Tivoli notice. Change icon. Popup alarm.
Compare Files:				
Daemon Status:				
amd	Critical	Becomes unavailable		Send Tivoli notice. Change icon. Popup alarm.
biod	Critical	Becomes unavailable		Send Tivoli notice. Change icon. Popup alarm.
cron	Critical	Becomes unavailable		Send Tivoli notice. Change icon. Popup alarm.
inetd	Critical	Becomes unavailable		Send Tivoli notice. Change icon. Popup alarm.
lockd	Critical	Becomes unavailable		Send Tivoli notice. Change icon. Popup alarm.
lpd	Critical	Becomes unavailable		Send Tivoli notice. Change icon. Popup alarm.

mountd	Critical	Becomes unavailable		Send Tivoli notice. Change icon. Popup alarm.
nfsd	Critical	Becomes unavailable		Send Tivoli notice. Change icon. Popup alarm.
portmap	Critical	Becomes unavailable		Send Tivoli notice. Change icon. Popup alarm.
snmpd	Critical	Becomes unavailable		Send Tivoli notice. Change icon. Popup alarm.
statd	Critical	Becomes unavailable		Send Tivoli notice. Change icon. Popup alarm.
File Checksum:				
/etc/passwd	Warning	Not equal to	value	Change icon.
File Size:				
/var/adm/messages	Warning	Greater than	200 Kbytes	Change icon.
Occurrences in File:				
/var/adm/messages	Warning	Greater than	value	Change icon.
Process Instances:				
tivoli	Warning	Greater than	3	Change icon.
HP OpenView	Warning	Greater than	3	Change icon.
User Logins by User:				
root	Warning	Greater than	1	Change icon.
Users Logged in	Warning	Greater than	20	Change icon.
	Severe	Greater than	25	Send Tivoli notice. Change icon.
	Critical	Greater than	30	Send Tivoli notice. Change icon. Popup alarm.

Table 7.2-3 Network Event Configuration

Resource	**Response Level**	**Trigger When**	**Threshold**	**Response**
Client RPC timeouts	Warning	% increase of	10	Change icon.
	Severe	% increase of	25	Send Tivoli notice. Change icon.
	Critical	% increase of	50	Send Tivoli notice. Change icon. Popup alarm.
Server Status				
Network Collisions	Warning	% increase of	5	Change icon.
	Severe	% increase of	10	Send Tivoli notice. Change icon.
	Critical	% increase of	25	Send Tivoli notice. Change icon. Popup alarm.
Network Collisions/packets	Warning	% increase of	5	Change icon.

	Severe	% increase of	10	Send Tivoli notice. Change icon.
	Critical	% increase of	25	Send Tivoli notice. Change icon. Popup alarm.
NFS bad calls	Warning	% increase of	10	Change icon.
	Severe	% increase of	25	Send Tivoli notice. Change icon.
	Critical	% increase of	50	Send Tivoli notice. Change icon. Popup alarm.
Input packet errors	Warning	% increase of	10	Change icon.
	Severe	% increase of	25	Send Tivoli notice. Change icon.
	Critical	% increase of	50	Send Tivoli notice. Change icon. Popup alarm.
Input packets	Warning	% increase of	10	Change icon.
	Severe	% increase of	25	Send Tivoli notice. Change icon.
	Critical	% increase of	50	Send Tivoli notice. Change icon. Popup alarm.
Output packet errors	Warning	% increase of	10	Change icon.
	Severe	% increase of	25	Send Tivoli notice. Change icon.
	Critical	% increase of	50	Send Tivoli notice. Change icon. Popup alarm.
Output packets	Warning	% increase of	10	Change icon.
	Severe	% increase of	25	Send Tivoli notice. Change icon.
	Critical	% increase of	50	Send Tivoli notice. Change icon. Popup alarm.
Remote oserv status	Critical	Becomes unavailable		Send Tivoli notice. Change icon. Popup alarm.
RPC bad calls	Warning	% increase of	10	Change icon.
	Severe	% increase of	25	Send Tivoli notice. Change icon.
	Critical	% increase of	50	Send Tivoli notice. Change icon. Popup alarm.

Table 7.2-4 System Event Configuration

Resource	**Response Level**	**Trigger When**	**Threshold**	**Response**
Available swap space	Warning	Less than	20 MB	Change icon.

	Severe	Less than	15 MB	Send Tivoli notice. Change icon.
	Critical	Less than	10 MB	Send Tivoli notice. Change icon. Popup alarm.
Host status:				
cyclops	Critical	Becomes unavailable		Send Tivoli notice. Change icon. Popup alarm.
Lingering terminated processes	Warning	Greater than	10	Change icon.
	Severe	Greater than	20	Send Tivoli notice. Change icon.
	Critical	Greater than	30	Send Tivoli notice. Change icon. Popup alarm.
Load average	Warning	Greater than	10	Change icon.
	Severe	Greater than	20	Send Tivoli notice. Change icon.
	Critical	Greater than	30	Send Tivoli notice. Change icon. Popup alarm.
Mail queue length	Warning	Greater than	20	Change icon.
	Severe	Greater than	40	Send Tivoli notice. Change icon.
	Critical	Greater than	50	Send Tivoli notice. Change icon. Popup alarm.
Page-outs	Warning	% increase of	50	Change icon.
	Severe	% increase of	80	Send Tivoli notice. Change icon.
	Critical	% increase of	90	Send Tivoli notice. Change icon. Popup alarm.

Table 7.2-5 Printer Event Configuration

Resource	**Response Level**	**Trigger When**	**Threshold**	**Response**
Daemon status:				
lpsched	Critical	Becomes unavailable		Send Tivoli notice. Change icon. Popup alarm.
Jobs in print queue:				
print_queue	Warning	Greater than	10	Change icon.
Status of print queue:				

print_queue	Critical	Becomes unavailable		Send Tivoli notice. Change icon. Popup alarm.
Total size queued:				
print_queue	Warning	Greater than	10 M	Change icon.
	Severe	Greater than	20 M	Send Tivoli notice. Change icon.
	Critical	Greater than	30 M	Send Tivoli notice. Change icon. Popup alarm.

X - system dependent parameters.

8. Problem Management

The Trouble Ticket System is the vehicle to record and report M&O problems during the operational phase. Trouble tickets can be generated by operations, maintenance, development, and customer personnel as well as users. The Trouble Ticket System is wholly automated and all problem resolution activities are recorded in the database tool, the Remedy Action Request System. Documentation that is not in electronic form is handled by the local CM Administrator (CMA) and is listed as an attachment to the trouble ticket.

A CM Administrator (site or system-level) is assigned to serve as a Trouble Ticket database administrator. The CMA is responsible for tracking ECS system-level issues discovered at the sites and for propagating system problem resolutions to the site level. The CMA also supports the activities of the Trouble Ticket Review Board. This includes generating status reports, and distributing resolutions, instructions, and changes as directed by the Board. User Services Representatives monitor trouble tickets to notify users concerning problem resolution and status. Maintenance engineers record all activities in the trouble ticket. This information can be used to determine critical maintenance concerns related to frequency of occurrence, criticality level, and the volume of problems experienced. The maintainability analysis will guide critical changes, volume and type of support components to be utilized, and will focus further ECS release development.

This section provides an overview of the Trouble Ticketing process and defines the M&O procedures for processing and resolving trouble ticket submissions. In addition, this section provides instructions for diagnosing network problems.

8.1 Problem Resolution Process — An Overview

External users submit trouble tickets to the User Services Desk through the Internet [using a series of hypertext mark-up language (HTML) screens (see Section 8.3, below). DAAC personnel submit trouble tickets via Remedy.

Trouble tickets are first evaluated by the Ops Supervisor to determine the severity and cause of the problem as the basis for assignment of priority and on-site responsibility/cognizance. Every trouble ticket is logged into the database for record keeping purposes. Trouble tickets that can be resolved locally are assigned and tracked at the local center. Matters of sufficient importance are escalated to the Trouble Ticket Telecon agenda for further discussion and disposition.

Trouble Tickets are discussed at a weekly trouble ticket Telecon. This meeting functions as the ECS Failure Review Board in compliance with the *EOS Performance Assurance Requirements for ECS*, GSFC 420-05-03, Section 7.12.2.2. The telecon is held to coordinate trouble ticket activities within the system and site M&O organization as well as with development, customer, and user organizations. Attendees include: Customer representatives; ECS SEO engineering teams leads (one is designated as chairperson of the meeting); ECS ILS engineering support; ECS engineering team leads and operations representatives; ECS M&O support staff; ECS development

organization representatives (including management, technical, configuration management and quality assurance); SCF(s) representatives.

Agenda items may be supplemented or replaced by hardcopy or softcopy reports. Material from this meeting is distributed within each ECS organization and to customer and user organizations as required. A typical agenda might include:

- Review and prioritize (system-level) each trouble ticket opened at each center.
- Review and re-prioritize older trouble tickets (as required).
- Assign trouble ticket work-off responsibility to one organization.
- Review distribution of trouble tickets by organization, priority and age.
- Discuss trouble ticket issues with development organizations.

The Maintenance & Operations Problem Management Concept is outlined in the following procedures, which are illustrated in Figures 8.1-1 and 8.1-2:

1. User or Operator discovers a problem with ECS configuration item(s) (hardware, software, documentation, procedure) and documents this problem for later resolution. A user submits to User Services: by calling up the Trouble Ticket System via the Internet (see Section 8.3, below); by going on-line with the Trouble Ticket database (Remedy) ; by phoning User Services; or by sending an e-mail message to Remedy. (See Section 8.2.2.) Operators document problems directly via Remedy.

2. The trouble ticket is logged into the system. Remedy automatically assigns "New" status to the trouble ticket and notifies the Operations Supervisor for assignment and prioritization. Remedy notifies the Operations Supervisor via email, or through Remedy's notification tool, or both (see Section 8.2.1.4). Trouble tickets are subsequently statused and reported by the CMA.

3. The trouble ticket log is prioritized according to a triage system of maintenance priorities which will be determined in relation to the effect of a problem on mission success which shall be differentiated by scope of impact, frequency of occurrence, and the availability of an adequate work-around. The Performance Assurance Requirements document, NASA 420-05-03, identifies problem categories which correspond to the triage system of maintenance priorities:

Category 1: System/Service cannot perform critical function or imposes major safety hazard. (Priority 1)

Presents an immediate impact to development, operations, services, or data processing functions; imposes major safety hazard to personnel, systems, or space mission resources; or results in loss of one or more essential mission objectives.

Category 2: System/Service substantially impaired. (Priority 2)

Substantially impacts development, operations, services, or data processing functions; fails to operate within critical performance specifications; or cannot effectively or efficiently fulfill baseline requirements.

Category 3: System/Service slightly impaired. (Priority 3)

Causes minor or no substantial impact to development, operations, services, or data processing functions. Support may be degraded, but mission can still be accomplished.

The Trouble Ticket System tool (Remedy) has coded the triage as HIGH, MEDIUM, and LOW. The User can designate a priority level for the problem. However, the official priority is assigned by the Operations Supervisor and maintained by the CM Administrator. All Category 1 (Priority 1) trouble tickets will be elevated to the Government Failure Review Board and will require both Government and Contractor Project Manager approval for final close-out. The sites and SEO apply these additional priorities:

Priority 4: Nuisance Problem: Includes the arrangement of video screens, color, and so on.

Priority 5: Closed Problem: A known issue with a prior disposition.

4. All affected Operations Supervisors at the sites (SMC, DAACs, EOC, EDF) are notified of the problems with potential system impact and may provide inputs to problem assessment (impact) and resolution.

5. The Trouble Ticket database is updated with inputs received by the Operations Supervisor, and the trouble ticket may be modified to reflect this new information/coordination activity.

6. The Operations Supervisor assigns the problem to a Problem Investigator for further follow-up.

7. The Problem Investigator is responsible for problem investigation, proposed resolution and coordinates input from SEO, developers, vendors, and external organizations to effect the local resolution. The Problem Investigator presents significant issues at the contractor Telecon sponsored by SEO.

8. The Problem Investigator updates the trouble ticket database.

9. The Problem Investigator forwards any information regarding proposed/implemented fixes to the established notification list.

10. The proposed resolution is then presented to the Trouble Ticket Review Board (and Government Failure Review Board for Priority 1 and Priority 2 problems) for review, ratification, or revision.

11. Changes that do not affect configuration controlled items may be approved and implemented by the Failure Review Board/Trouble Ticket Review Board and closed. CCBs must approve changes that affect configuration controlled items. Temporary changes are updated in Baseline Manager (see Section 9.9 of this document). Permanent changes are proposed in a CCR to either on-site or system-level CCBs. Emergency fixes can be made and then reported to the CCB after the crisis is resolved. (See Section 8.4.)

12. The CCBs may approve, reject, or revise the change proposal.

13. The on-site Trouble Ticket Review Board may revise the proposed solution.

14. The off-site problem resolution process will be managed by the SEO Trouble Ticket Review Board, who may also revise the on-site proposed solution because of any system-level effect(s). This is part of the problem escalation process which also includes appropriate submission of CCR(s).

15. The CCR may be escalated to higher level CCBs for system and/or external elements that may be involved in the resolution process.

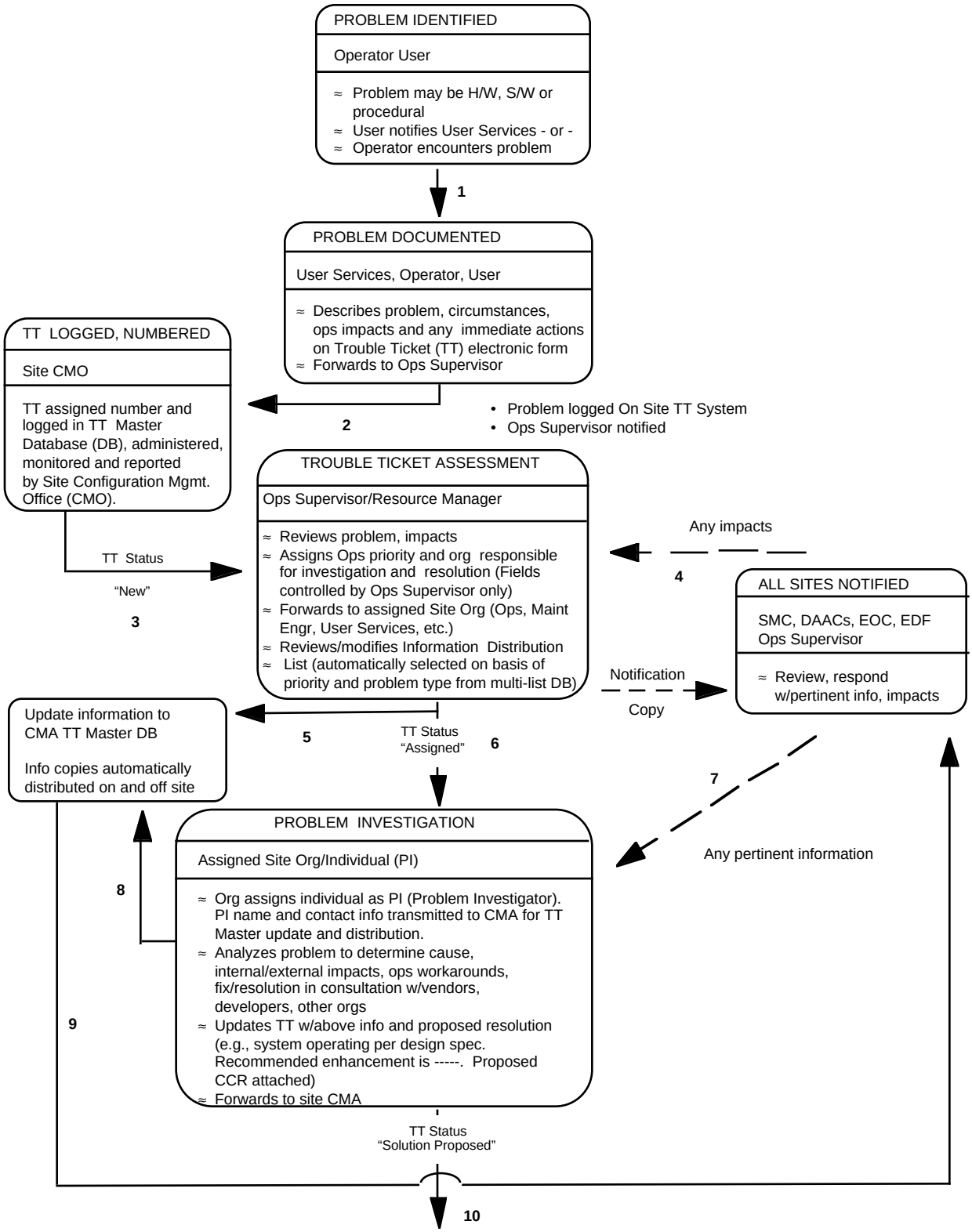

Figure 8.1-1 ECS Problem Management Concept - Part I

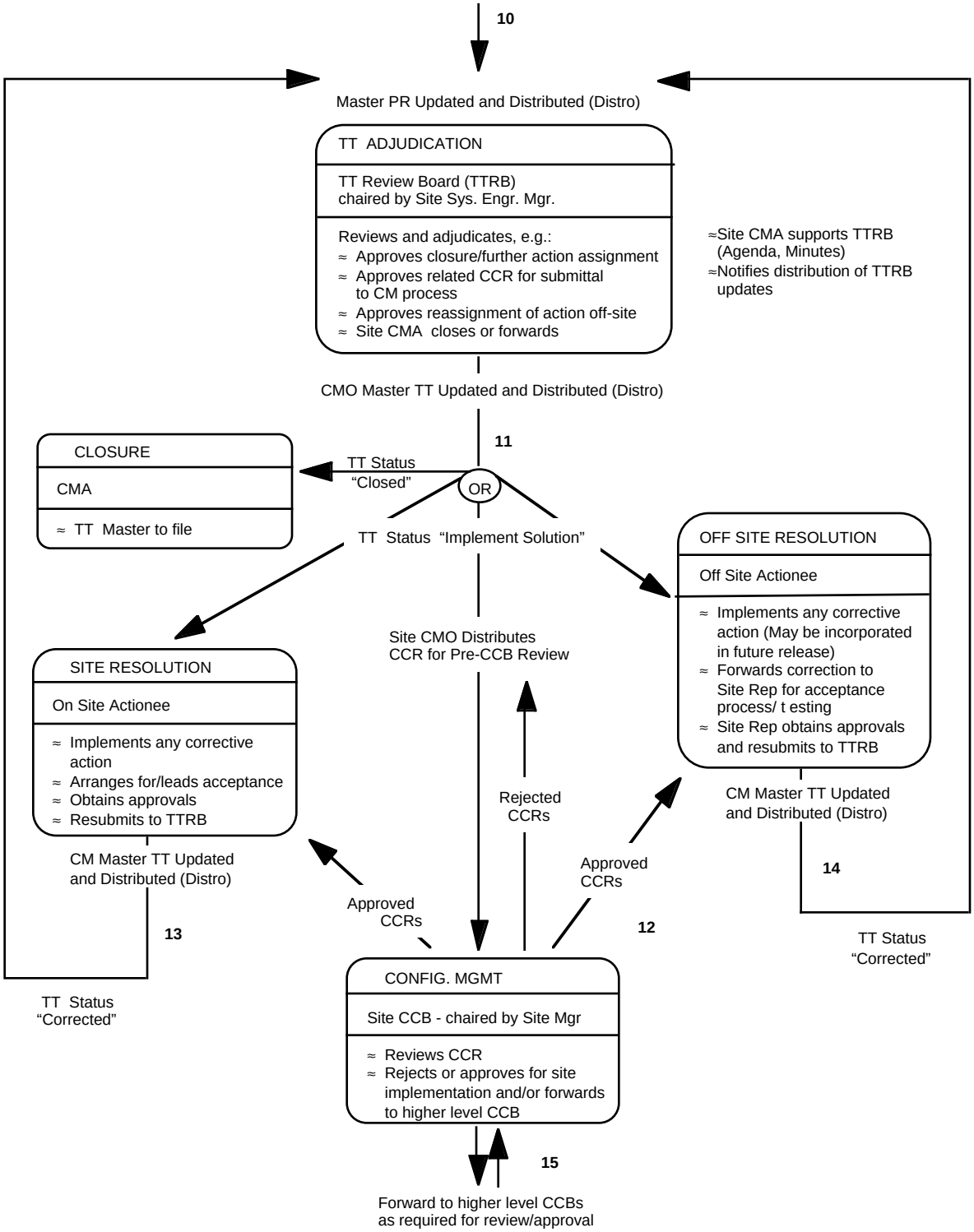

Figure 8.1-2 ECS Problem Management Concept - Part II

8.2 Using the Trouble Ticket System Tool

The Remedy Action Request System provides a distributed Trouble Ticketing Service that furnishes DAACs a common environment and means of classifying, tracking, and reporting problem occurrence and resolution to both ECS users and operations personnel. The Trouble Ticketing Service:

- Provides a GUI for operations personnel to access all Trouble Ticket services.
- Provides a common Trouble Ticket entry format.
- Stores Trouble Tickets.
- Retrieves Trouble Tickets via ad hoc queries.
- Allows operations personnel to forward problems from one site to another.
- Produces stock and common reports.
- Interfaces with user's and operator's e-mail to provide automatic notification.
- Offers an application programming interface through which applications can submit trouble tickets.
- Provides summary information to the SMC from each DAAC to allow trend reports regarding trouble tickets.
- Defines a consistent "life cycle" for trouble tickets.
- Allows each DAAC a degree of customization through definition of further re-prioritization and action rules.

Rules for re-prioritization are time-activated events, which execute on trouble tickets that meet a set of specified criteria (see Section 8.2.9, below). Actions which can be taken include notification (either to a user or to a support staff member), writing to a log file, setting a field value on the trouble ticket, or even running a custom written process. Qualifications can be expressed on any trouble ticket data tracks. Active links are similar to escalation rules with the exception that they are defined to take place on a specified action rather than at a given time.

In addition to the functionality provided by Remedy's Action Request System, the Trouble Ticketing Service utilizes a set of custom HTML pages ("screens") to provide registered users with the ability to submit new trouble tickets and query the current status of any of their previous entries. Access to the Trouble Ticketing System through this technique provides users an easy method for reporting problems in an environment with which most are already familiar. (See Section 8.3, below.) Additionally, as another means of trouble ticket entry, the Trouble Ticket System provides a text e-mail template through which automated entry of trouble tickets is possible. Support staff members are able to enter Trouble Tickets through the Remedy's Action Request System interface for problems received via other methods (for example, phone calls).

In addition to tracking trouble tickets, the Remedy Action Request System also functions as the User Contact Log. Remedy's Action Request System is configured to have a separate schema that contains the entries that User Services personnel enter for each contact that they receive from a user. The User Contact Log allows a trouble ticket to be initiated from a log entry with the push of a button — the Trouble Ticket will be populated with information from the contact log.

Sections 8.2.1 through 8.2.9 provide procedures using HTML and Remedy. If you need more information about using HTML, see Section 8.3, below. For more information using Remedy, see the Remedy User's Guide.

The Activity Checklist table that follows provides an overview of the Trouble Ticket System. Column one (**Order**) shows the order in which tasks might be accomplished. Column two (**Role**) lists the Role/Manager/Operator responsible for performing the task. Column three (**Task**) provides a brief explanation of the task. Column four (**Section**) provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found. Column five (**Complete?**) is used as a checklist to keep track of which task steps have been completed.

Table 8.2-1 Trouble Ticket System - Activity Checklist

Order	Role	Task	Section	Complete?
1	ECS users	Access the Trouble Ticket System	8.2.1, 8.3.1	
2	ECS users	Submit Trouble Ticket	8.2.2	
3	Maintenance Engineer	Modify Open Trouble Ticket	8.2.3	
4	Operations Supervisor, Maintenance Engineer	Forward Trouble Ticket	8.2.4	
5	Database Administrator	Add Users to Remedy	8.2.5	
6	CMA	Modify Remedy User Privileges	8.2.6	
7	CMA	Modify Remedy's Configuration	8.2.7	
8	Maintenance Engineer, CMA	Generate Reports	8.2.8	
9	Maintenance Engineer	Maintain Escalation Time Table	8.2.9	

8.2.1 Accessing the Trouble Ticket System

The Trouble Ticket System is accessed through either HTML or Remedy. The Trouble Ticket HTML is used by both User Services and the end user to submit trouble tickets without going through Remedy. It is accessed by clicking on the Trouble Ticket icon. Through HTML, the user can submit, obtain a list, and view details of trouble tickets.

Through Remedy, the User clicks on the User Tool icon, which opens the RelA-Trouble Tickets schema to submit, query, or work a Trouble Ticket. The Main Remedy Trouble Ticket screen is used to select the appropriate schema for submitting, modifying, or displaying a trouble ticket. The Main Page data fields are identified in Table 8.2-2.

The RelA-Trouble Tickets Schema provides the following options, which are initiated by clicking on the appropriate button:

- **Forward** -- Forwards this Trouble Ticket to the site specified in the "Forward-to" field.
- **Hardware Information** -- Opens a window that is associated with this Trouble Ticket to hold hardware information. (See Section 8.2.1.3.)
- **List All Masters** -- All Trouble Tickets that are duplicates of each other have one master. This button will lists all master Trouble Tickets.
- **List This Trouble Ticket's Duplicate(s)** -- List all Trouble Tickets that have duplicates associated to this Trouble Ticket.
- **Go to Contact Log** -- If this Trouble Ticket was created from a Contact Log, then this button will open a window to that Contact Log.

Several time-saving features are available through Remedy: the Admin Tool, GUI Import tool, the Hardware Information schema, and the GUI Notification tool. Brief descriptions are provided in Sections 8.2.1.1 through 8.2.1.4.

Table 8.2-2 RelA-Trouble Ticket Field Description

Field Name	Data Type	Size	Entry	Description
Ticket-Id	Character	15	System generated	Ticket number which is set and maintained by the system
Ticket Status	Selection	4	Required	Status of the Trouble Ticket
Assigned-Priority	Selection	4	Required	Priority of Trouble Ticket assigned at the site (HIGH, MEDIUM, LOW)
Short Description	Character	128	Required	Short Description of the problem
Submitter Impact	Selection	4	Optional	Impact of the problem to the submitter
Long-Description	Character	255	Optional	Long Description of the problem
Resolution Log (End	Diary	Unlim	Optional	General steps in the resolution of

User Sees)				the problem
Detailed Resolution Log	Diary	Unlim	Optional	Detailed steps in the resolution of the problem
Submitter ID	Character	30	Required	User Id of the Submitter.
Submitter Name	Character	30	Optional	Full Name of the Submitter
Submitter Phone	Character	30	Optional	Phone number of the Submitter
Submitter eMail	Character	64	Optional	E-mail address of the Submitter
Submitter Home DAAC	Character	60	Optional	Home DAAC of the Submitter
History	Diary	Unlim	Optional	Upon submission or modification, the person assigned to the ticket and the ticket status will be indicated in the History field. Due to a limitation in Remedy, this information will only be written when the Assigned-to and Status fields are modified
Assigned-To	Character	30	Optional	Person that Trouble Ticket has been assigned to
Last-modified-by	Character	30	System generated	Person that last modified the Trouble Ticket
Create-date	Date/Time	4	System generated	Date Trouble Ticket was created at the present site
Last-Modified-date	Date/Time	4	System generated	Date the Trouble Ticket was last modified
Related CCR	Character	60	Optional	ID of a related CCR
Key Words	Character	255	Optional	Key words to help identify this Trouble Ticket
Problem Type	Character	30	Optional	Type of problem addressed by this Trouble Ticket
Closing Code	Character	60	Optional	Origin of the problem that this Trouble Ticket resulted from
Closed-by	Character	60	Optional	Person that closed this Trouble Ticket
Close-date	Date/Time	4	Optional	Date this Trouble Ticket was closed
Software Resource	Character	60	Optional	Software Resource that the problem came from
Hardware Resource	Character	60	Optional	Hardware Resource that this problem came from
Duplicate Master Id	Character	25	Optional	The Master Ticket-ID of this Trouble Ticket
Forward-to	Character	60	Optional	Site that this Trouble Ticket was last forwarded to
Forwarded-from	Character	60	Optional	Site that forwarded this Trouble Ticket
Forwarded-by	Character	60	Optional	Contact person at the forwarding

				site
Forward-date	Date/Time	4	Optional	Date Trouble Ticket was forwarded
Unique-Identifier	Character	20	Optional	Unique identifier which is established at the origination site This identifier should NEVER be changed once set
Forwarded-to-1	Character	60	Optional	First site to have been forwarded this Trouble Ticket
Forwarded-to-2	Character	60	Optional	Second site to have been forwarded this Trouble Ticket
Forwarded-to-3	Character	60	Optional	Third site to have been forwarded this Trouble Ticket
Forwarded-to-4	Character	60	Optional	Fourth site to have been forwarded this Trouble Ticket
Associated Contact Log Id	Character	30	Optional	ID number of the Associated Contact Log

8.2.1.1 Remedy's GUI Admin Tool

The Admin Tool is used to notify or set fields as soon as the trouble ticket reaches a particular state or to escalate the problem once a trouble ticket is in a particular state too long. This tool is accessed in two ways:

1. By clicking on Admin Tool to open correct filter, escalation, or active link. (Problem escalation is discussed in Section 8.2.9.)
2. By clicking on User Tool icon and opening RelA-TT-Times schema to review/modify a Trouble Ticket.

For more information on the Admin Tool, refer to the Remedy Administration Manual.

8.2.1.2 Remedy's GUI Import Tool

The GUI Import tool is used to import existing entries rather than retyping information manually. It also enables the user to import entries into a schema from a file generated by the Admin tool. This tool is accessed by clicking on the Remedy Import Tool icon. For more information on the Import tool, refer to the Remedy User Guide.

8.2.1.3 Remedy's Hardware Information Schema

If detailed hardware information needs to be provided beyond what can be entered on the Trouble Tickets schema. The User Tool, Hardware Information schema, provides the vehicle to add a description of a hardware problem that corresponds to a trouble ticket. Through this schema, the user can enter detailed information about failed hardware components (e.g., part and serial numbers) and the actions taken to correct the problem. This schema is accessed by clicking on the User Tool icon and opening RelA-Hardware Information schema, or via Hardware Information link from Trouble Tickets schema.

8.2.1.4 Remedy's GUI Notification Tool

The GUI Notification Tool is used as an alternative to email notification to notify the user of a Remedy event. This tool is accessed by clicking on the Remedy Notification Tool icon. It allows properties and options to be modified via pull-down menus. Examples of GUI notification include a beep, a pop-up window, a flashing message. In addition, both an email and a GUI notification can be sent if the site so desires.

8.2.2 Submit a Trouble Ticket

When a problem is either found by or reported to User Services, follow the procedure applicable to your system, to create and log trouble tickets. Trouble tickets can be submitted via HTML or via Remedy's user tool – RelA-Trouble Tickets schema. Remedy's Contact Log schema is used to classify, track, and report contacts of ECS users and operators and also to submit a trouble ticket from a log entry. E-mail is another method of submitting a trouble ticket. The template is available from your System Administrator.

1. For HTML submission:

    a) Access HTML Trouble Ticketing Main page. Click on Trouble Ticket icon from the ECS desktop.

    b) Select Submit link which opens the Submit page.

    c) Fill out the impact, short description, and detailed description fields.

    d) Select Submit.

2. For submission through Remedy (See the Remedy User Guide, Chapter 3, “Submitting an Action Request” for the general steps):

    a) Access Remedy User Tool (See the Remedy User Guide, Chapter 2, “Getting Started with the User Tool”, page 2-3, section on “Starting the User Tool”).

    b) Access RelA-Trouble Ticket schema (See the Remedy User Guide, Chapter 2, “Getting Started with the User Tool”, page 2-18, section on “Using Schemas”).

    c) Select Open Submit from the File menu.

    d) Fill out at least Short Description and User Identification.

    e) Fill out any other pertinent fields.

    f) Select Apply.

3. For submission from a Remedy Contact Log entry:

    a) Click on User Tool icon and open RelA-Contact Log schema.

    b) Fill out Contact Log ID and Contact Information. If the contact is a registered Remedy user, the contact information is filled out automatically.

c) Fill in Short Description (limit is 128 characters).

d) Click on **Create TT** button.

4. For submission via E-mail:

a) Obtain Template from your System Administrator.

b) Address the message to arsystem@_____._____._____.

c) Copy template into message area. DO NOT INCLUDE AS AN ATTACHMENT. DO NOT ALTER TEMPLATE. The template is presented in Figure 8.2.2-1. The # sign indicates comments, which are not read by Remedy. **Enter data as indicated in Figure 8.2.2-1.** Send message.

```
#
#  File exported Wed Feb 28 19:01:27 1996
#
Schema: RelA-Trouble Tickets
Server: remedy server name
Login:
Password:

       Short Description !        8!:
        Submitter Impact !536870922!: Low
# Values: Low, Medium, High
        Long-Description !        9!:
            Submitter ID !        2!:
          Submitter Name !536870917!:
         Submitter Phone !536870918!:
         Submitter eMail !536870921!:
     Submitter Home DAAC !536870919!:
```

Field ID internal to Remedy

Default value

Select one

Enter data after colon

Figure 8.2-1 Trouble Ticket E-mail Template

8.2.3 Reviewing and Modifying Open Trouble Tickets

Trouble tickets may need to be modified based on better understanding of the nature of problems defined and revised resolutions from the Maintenance Engineer investigations, Sustaining Engineering inputs, Developer inputs, Trouble Ticket Review Board decisions, Change Control Board decisions, and/or Failure Review Board decisions. The results will be factored into revisions and/ or additions to the Trouble Ticket log.

1. For HTML Review and Modification of Trouble Tickets:

a) Access HTML Trouble Ticketing Main (see Section 8.3). Trouble Tickets can be ***submitted, queried or modified***.

b) Select List link which opens the List page and shows each Trouble Ticket's Identification, Short Description, and Status.

c) Select the Trouble Ticket Id to get a more detailed description of that particular Trouble Ticket.

2. For Reviewing and Modifying Trouble Tickets through Remedy (See the Remedy User Guide, Chapter 4, "Reviewing and Modifying Action Request" for the general steps):

a) Access Remedy User Tool (See the Remedy User Guide, Chapter 2, "Getting Started with the User Tool", page 2-3, section on "Starting the User Tool").

b) Access Release A-Trouble Ticket schema (See the Remedy User Guide, Chapter 2, "Getting Started with the User Tool", page 2-18, section on "Using Schemas").

c) Select List from the Query menu.

d) From the List pick the Trouble Ticket(s) that you would like to Review/Modify.

e) Select Modify Individual from the Query menu of the List window review and modify Trouble Ticket.

8.2.4 Forwarding Trouble Tickets

Trouble ticket administrative reports are forwarded for local and system-wide usage. The trouble ticket contains all forwarding information; once forwarded, it goes to the RelA-TT-ForwardToSite holding area (transparent to the user). The RelA-TT-Sites schema is used to indicate the site name and email address to be used in forwarding. To forward a trouble ticket:

1. Click on User Tool icon and open RelA-Trouble Ticket schema.
2. Set the status to "Forwarded".
3. Select a value for the Forward-to field from its picklist.
4. Select the Forward button.
5. Select Apply.

If necessary, a site name and email address can be modified, added, or deleted to update the picklist of Release A sites by authorized Remedy users: DAACs, SMC, NSI, EBnet. To modify picklist:

1. Click on User Tool icon and open RelA-TT-Sites schema.
2. Modify data.

8.2.5 Adding Users to Remedy

The database administrator uses the RelA-User schema to grant access to the Remedy tool. See Remedy Administrator's Guide for OSF/ Motif, Chapter 3, "Setting Up Users and Groups", page 3-11, section on "Adding Users". Users who change jobs can be deleted.

8.2.6 Changing Privileges in Remedy

This procedure is used by the CM Administrator to control privileges of those who have been granted access. For more information, refer to the Remedy Administrator's Guide.

NOTE: No group should be modified without proper configuration change approval.

To change Privileges in Remedy:

1. See Remedy Administrator's Guide, Chapter 3, "Setting Up Users and Groups", page 3-2, section on "Understanding Access Control".
2. See Remedy Administrator's Guide, Chapter 3, "Setting Up Users and Groups", page 3-4, section on "Access Control Groups".
3. Groups have already been created to accommodate all privileges needed by Remedy Users for Release A. These groups are identified in see Table 8.2-3.

Table 8.2-3 Table of Access Control Groupings

Groups	Description	Access Type
Operator	Submits trouble ticket internally.	Change
User Services	Submits trouble ticket internally for user.	Change
Operations Supervisor	Assigns problem priority and resolution responsibility. Can forward trouble ticket to another site.	Change
Resource Manager	Assigns problem priority and resolution responsibility. Can forward trouble ticket to another site.	Change
Resolution Technician	Attempts to resolve problem.	Change
Trouble Ticket Review Board Chair Person	Reviews proposed solutions	Change
Administrator	Adds groups and users. Changes permissions. Sets escalation times. Sets menu items. Etc.	Change
Sub-Administrator	Same functions as Administrator but only with certain Schemas.	Change
Browser	Read only permission.	Read
Customize	Can use all features of the customize facility.	Change
Submitter	Place holder for anyone that submits a trouble ticket.	NA
Assignee	Place holder for anyone that is assigned a trouble ticket.	NA
Public	Read only permission. Guest users are automatically put in this group.	Read
NotifyNewEscal	Everyone that will be notified on an escalation due to trouble ticket being in "New" status.	Read

Groups	Description	Access Type
NotifyAssignedEscal	Everyone that will be notified on an escalation due to trouble ticket being in “Assigned” status.	Read
NotifySolPropEscal	Everyone that will be notified on an escalation due to TT being in “Solution Proposed” status.	Read
NotifyImpSolEscal	Everyone that will be notified on an escalation due to trouble ticket being in “Implement Solution” status.	Read
NotifySolImpEscal	Everyone that will be notified on an escalation due to TT being in “Solution Implemented” status.	Read

8.2.7 Modifying Remedy's Configuration

RelA-Trouble Ticket schemas' pulldown menus can be customized. Customization is achieved through the User Tool by modifying the RelA-Menu-Closing Codes, RelA-Menu-Hardware Resources, RelA-Menu-Software Resources, RelA-Menu-Key Words, RelA-Menu-Problem Type, Sites schemas.

To modify the Remedy environmental variables, refer to the Remedy User’s Guide and Remedy Administrator’s Guide as indicated.

1. See Remedy User’s Guide, Chapter 7, “Customizing the Environment.”

2. See Remedy Administrator’s Guide, Chapter 1, “Using the Administrator Tool.”

   NOTE: No administrative configuration should be made without proper configuration change approval.

8.2.8 Generating Trouble Ticket Reports

A set of predefined reports will be placed in a public directory that should be downloaded to your personal configuration directory (see the Remedy User Guide, Chapter 2, “Getting Started with the User Tool,” page 2-31, section “Sharing Macros, User Commands and Custom Reports,” sub-section “Copying Files”). These reports are trouble ticket administrative reports generated for local and system-wide usage. See Remedy User’s Guide, Chapter 5, “Reports.”

8.2.9 Re-prioritization of Dated Trouble Ticket Logs

Remedy provides automated prioritization of trouble tickets based on delinquency status of out-dated trouble ticket logs. The File Tickler System automatically assigns higher priority to promote timely resolution.

1. Access Remedy User Tool (See the Remedy User Guide, Chapter 2, “Getting Started with the User Tool,” page 2-3, section on “Starting the User Tool”).

2. Access RelA-Times schema (See the Remedy User Guide, Chapter 2, “Getting Started with the User Tool”, page 2-18, section on “Using Schemas”).

3. Select List from the Query menu.

4. From the List pick the Time(s) that you would like to Review/Modify.

5. Select Modify Individual from the Query menu of the List window to review and/or modify the Time (in seconds).

8.3 Using Hypertext Mark-up Language (HTML) Screens

The hypertext mark-up language (HTML) Trouble Ticket Main Screen ("ECS Trouble Ticketing: Menu") provides an introduction on how to use the Trouble Ticketing HTML, and is used by registered ECS users to go to either the Submit page or List page.

Selecting **Submit a Trouble Ticket** will bring up the Trouble Ticketing Submit screen.

Selecting **List the [username] Trouble Tickets** will bring up the Trouble Ticketing List screen.

Help on the Trouble Ticket HTML screens is available by clicking on the Trouble Ticket Help icon at the bottom of the screen .

8.3.1 ECS Trouble Ticketing HTML Submit Screen

The HTML Trouble Ticket Submit screen is used by registered ECS users to submit a Trouble Ticket.

Table 8.3-1 below provides a description of the Trouble Ticket HTML Submit Screen fields.

Table 8.3-1 Trouble Ticket HTML Submit Screen Field Description

Field Name	Data Type	Size	Entry	Description
ID	character	30	System generated	Submitter Id
Name	character	30	System generated	Submitter Name
E-mail address	character	64	System generated	Submitter E-mail Address
Phone	character	30	System generated	Submitter Phone Number
Home DAAC	character	60	System generated	Submitter Home DAAC
Impact	selection	4	Required	Impact to Submitter
Short description	character	125	Required	Short description of problem
Detailed problem description	character	245	Optional	Long description of problem

When the information is completed, the user can submit the Trouble Ticket by clicking on the **Submit** button on the lower half of the screen. (The Success screen appears when a Trouble Ticket is successfully submitted. See Section 8.3.2 below.) The Problem Information Fields can be cleared by clicking on the **Reset** button. The user also has the choice of returning to the Trouble Ticketing Homepage or going to the Trouble Ticket Help screen by clicking on the respective icons at the bottom of the page.

8.3.2 ECS Trouble Ticketing HTML Success Screen

The HTML Trouble Ticket Success screen indicates a successful submission and reports the Trouble Ticket Id.

From this screen, the user is provided with the following information/options:

- Confirmation that the trouble ticket was successfully submitted, the trouble ticket identification number, and who submitted the trouble ticket.
- Notification that an E-mail message has been sent to the user indicating that a Trouble Ticket has been submitted and when it was closed. Selecting this Trouble Ticket will open the Trouble Ticket Detailed Screen.
- Instructions telling the user how to check the progress of Trouble Ticket resolution.

The user also has the choice of returning to the Trouble Ticketing Homepage or going to the Trouble Ticket Help screen by clicking on the respective icons at the bottom of the page.

8.3.3 ECS Trouble Ticketing HTML List Screen

The HTML Trouble Ticket List screen is used by registered ECS users to List Trouble Tickets for a user and links the listed Trouble Ticket Number to the Trouble Ticket Detailed Screen.

Table 8.3-2 below provides a description of the Trouble Ticket HTML List Screen fields.

Table 8.3-2 Trouble Ticket HTML List Screen Field Description

Field Name	Data Type	Size	Entry	Description
Trouble Ticket Number	character	15	System generated	Trouble Ticket Id
Problem Short Description	character	125	System generated	Short Description of Problem
Status	character	20	System generated	Status of Trouble Ticket

The user also has the choice of returning to the Trouble Ticketing Homepage or going to the Trouble Ticket Help screen by clicking on the respective icons at the bottom of the page.

8.3.4 ECS Trouble Ticketing HTML Detailed Screen

The HTML Trouble Ticket Detailed screen is used by registered ECS users to see a more detailed output of a Trouble Ticket.

Table 8.3-3 below provides a description of the Trouble Ticket HTML Detailed Screen fields.

Table 8.3-3 Trouble Ticket HTML Detailed Screen Field Description

Field Name	Data Type	Size	Entry	Description
ID	character	30	System generated	Submitter Id
Name	character	30	System generated	Submitter Name
E-mail address	character	64	System generated	Submitter E-mail Address
Phone	character	30	System generated	Submitter Phone Number
Home DAAC	character	60	System generated	Submitter Home DAAC
Status	selection	4	System generated	Status of Trouble Ticket
Impact	selection	4	System generated	Impact to Submitter (low, medium, high)
Short description	character	125	System generated	Short description of problem
Detailed problem description	character	245	System generated	Long description of problem
Log	character	unlim.	System generated	Diary of problem resolution

The user also has the choice of returning to the Trouble Ticketing Homepage or going to the Trouble Ticket Help screen by clicking on the respective icons at the bottom of the page.

8.3.5 ECS Trouble Ticketing HTML Help Screen

The HTML Trouble Ticket Help screen is used by registered ECS users to get help with the HTML screens.

This screen provides general information on the following:

- Index -- links that scroll the screen to the Introduction, Submit Page, and List Page sections listed below.
- Introduction – provides information about the Trouble Ticket Help page
- Menu Page – describes the Trouble Ticketing Menu page.

- Submit Page – describes the Trouble Ticket Submit page.
- Success Page – describes the Trouble Ticket Success page.
- List Page – describes the Trouble Ticket List page.
- Detailed Page - describes the Trouble Ticket Detailed page.

8.4 Emergency Fixes

Any emergency may be dealt with on an ad hoc basis, but contingency plans, contact points for supervisors, responsible engineers, Sustaining Engineering Organization, vendors, and general guidelines need to be in place to provide a common framework for emergency response to crisis-level situations. Emergency fixes may have already been implemented on a temporary basis by the Trouble Ticket Review Board with concurrence from the CCB Chair who later receives the CCR to document/implement the permanent change. Urgent items will be reviewed by the next CCB meeting.